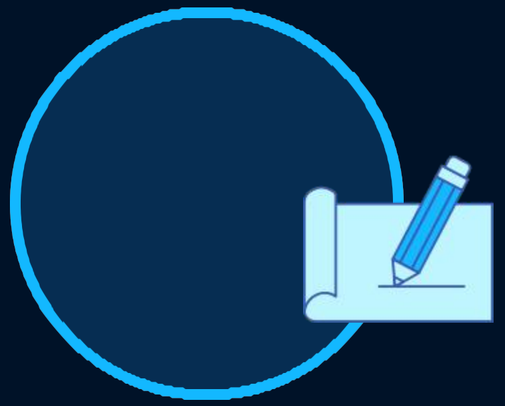
Senin, 02 September 2024

Manajemen Keamanan Informasi (ISO 27001)

Pertemuan Ke-1

Oleh: Nurmi Hidayasari



Kontrak Perkuliahan

Deskripsi MK

Teori: 1 SKS

Praktek: 2 SKS

Bobot Penilaian

UTS: 20%

UAS: 15%

Proses Praktikum: 50%

Laporan dan Tugas: 15%

Kedisiplinan

Pakaian rapi

Toleransi keterlambatan 15 menit

Dll (sesuai PA kampus)

CPL

Menguasai konsep dan mampu menerapkan analisis serta manajemen risiko keamanan informasi dalam konteks organisasi, termasuk identifikasi potensi risiko dan strategi mitigasi.

CPMK

- Mampu memahami dan menjelaskan struktur dan konsep dasar ISO 27001.
- Mampu merancang dan mengembangkan kebijakan keamanan informasi sesuai dengan ISO 27001.
- Mampu merancang dan mengimplementasikan kontrol keamanan informasi berdasarkan Annex A.
- Mampu menganalisis dan menilai risiko keamanan informasi serta mengembangkan langkah-langkah mitigasi.
- Mampu melakukan audit internal terhadap penerapan kebijakan keamanan informasi sesuai ISO 27001.
- Mampu mengelola hubungan dengan pemasok dan pihak ketiga terkait keamanan informasi.

Materi 1
Pengantar Standar SMKI SNI ISO/IEC 27001:2022

Standar

SMKI

SNI

Apa Itu Standar?

- Sepeda motor tidak ambruk;
- Secara sederhana memiliki fungsi untuk menopang beban kendaraan saat sedang parkir;
- Efisiensi ruang parkir;

Apa itu standar?

- Kepastian untuk pelanggan;
- Jaminan kepuasan pelanggan;
- Kemudahan ekspor;

Mengapa perlu standar ?

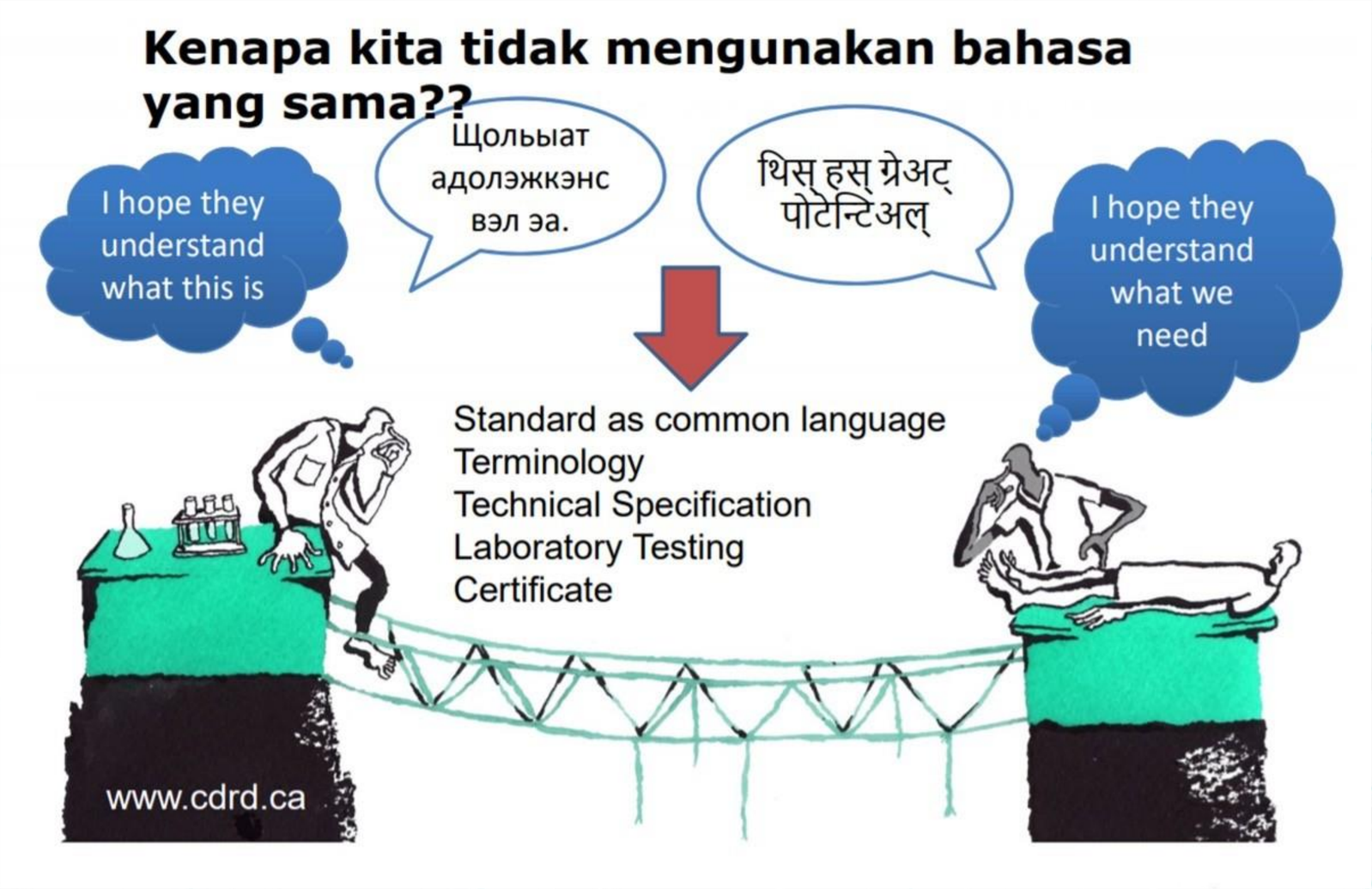
1. Sesuatu yang **aman** untuk manusia dan alam
2. Sesuatu yang **teratur, rapi dan indah**
3. Sesuatu yang **pasti**
4. **Timbangan** atau ukuran yang jelas
5. Birokrasi yang bersih **tidak korupsi** tidak menyuap
6. Sesuatu yang dapat **diklarifikasi, ditelusuri** dan **dikonfirmasi**
7. **Bahasa yang sama** atau platform/kluster yang sama
8. Sesuatu yang **hemat** (efisien dan efektif)
9. Sesutu yang memberikan **gambaran "mutu"**
10. **Perbaikan terus** (Continous improvement)-hari ini "lebih baik dari hari lain"
11. Kesepatan berbasis **musyawarah** dengan menindahkan agama budaya lingkungan kerarifan lokal IPTEK

Mengapa perlu standar ? (*lanjutan*)

- Melindungi konsumen, pelaku usaha dan masyarakat
- Meningkatkan jaminan mutu, efisiensi produksi, dan kemampuan pelaku usaha
- Bahasa dalam semua bidang, baik perdagangan, industri, pendidikan, dan pengujian
- Meningkatkan kepastian dan efisiensi transaksi perdagangan barang dan jasa baik dalam negeri maupun luar negeri
- Meningkatkan nilai dari suatu produk, jasa, penelitian di dalam negeri maupun luar negeri.

Dan lain-lain

Standar sebagai bahasa pengantar

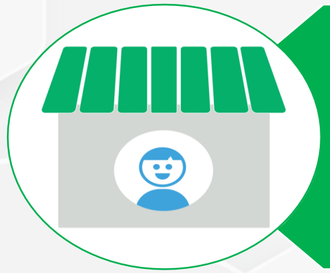


Definisi Standar Berdasarkan UU No. 20 SPK Tahun 2014

Standar adalah persyaratan teknis atau sesuatu yang dibakukan, termasuk tata cara dan metode yang disusun berdasarkan konsensus semua pihak/Pemerintah/keputusan internasional yang terkait dengan memperhatikan syarat keselamatan, keamanan, kesehatan, lingkungan hidup, perkembangan ilmu pengetahuan dan teknologi, pengalaman, serta perkembangan masa kini dan masa depan untuk memperoleh manfaat yang sebesar-besarnya.

Tujuan Standardisasi sesuai UU No. 20 Tahun 2014

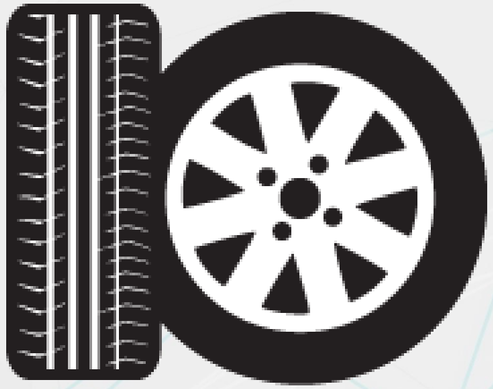
Meningkatkan **jaminan mutu, efisiensi produksi, daya saing nasional, persaingan usaha yang sehat** & **transparan** dalam perdagangan, kepastian usaha, dan kemampuan Pelaku Usaha, serta kemampuan **inovasi teknologi**;



Meningkatkan perlindungan kepada konsumen, Pelaku Usaha, tenaga kerja, dan masyarakat lainnya, serta negara, baik dari aspek keselamatan, keamanan, kesehatan, maupun pelestarian fungsi lingkungan hidup; dan

Meningkatkan **kepastian, kelancaran, dan efisiensi** transaksi perdagangan Barang dan/atau Jasa di dalam negeri dan luar negeri.

Contoh Standar



HTTP

Contoh Tidak Standar

SNI (Standar Nasional Indonesia)

Apa itu Sistem Manajemen

Kumpulan unsur yang saling berkaitan atau saling berinteraksi dari suatu organisasi untuk membuat kebijakan dan sasaran, dan proses untuk mencapai sasaran tersebut.

Apa itu Keamanan?

- ✓ Keadaan bebas dari bahaya
- ✓ Bebas dari gangguan
- ✓ Terlindungi
- ✓ Tidak dapat diambil orang

- KBBI -

Apa itu Informasi?

- ✓ Sesuatu (data) yang memiliki nilai (bisnis dan operasional) bagi organisasi.
- ✓ Sesuatu (data) yang kritikal bagi operasional organisasi.
- ✓ Infomasi adalah aset, seperti aset bisnis penting lainnya, yang memiliki nilai bagi suatu organisasi sehingga pada akhirnya perlu untuk diamankan.

Contoh Informasi

Informasi : Data Masyarakat data Karyawan, perjanjian dan kontrak, data keuangan

Perangkat Lunak : Aplikasi Office, Operating Sistem, Aplikasi Editing, Web aplikasi, Anti virus

Perangkat Keras : Komputer , Laptop, Switch , Printer

Sarana Pendukung : Listrik, Gedung, Jaringan Internet, Jaringan telepon

Sumber daya Manusia dengan keahliannya

5

Aset tidak Berwujud : Reputasi, Image Perusahan

Apa itu Keamanan Informasi?

Keamanan Informasi adalah Penjagaan terhadap Kerahasiaan (Confidentiality), Keutuhan (Integrity) dan Ketersediaan (Availability) atas informasi.

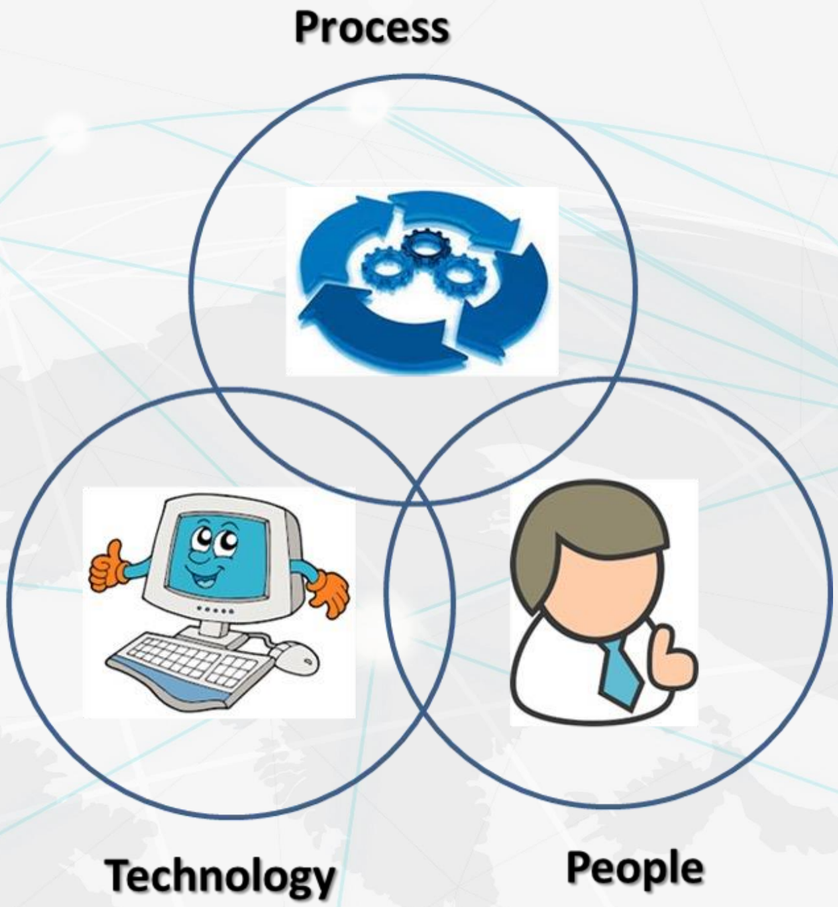
SNI ISO/IEC 27000:2018

Catatan : selain itu kontrol lain antara lain ***authenticity*** , ***accountability, non-repudiation*** dan ***reability*** juga dapat berpengaruh

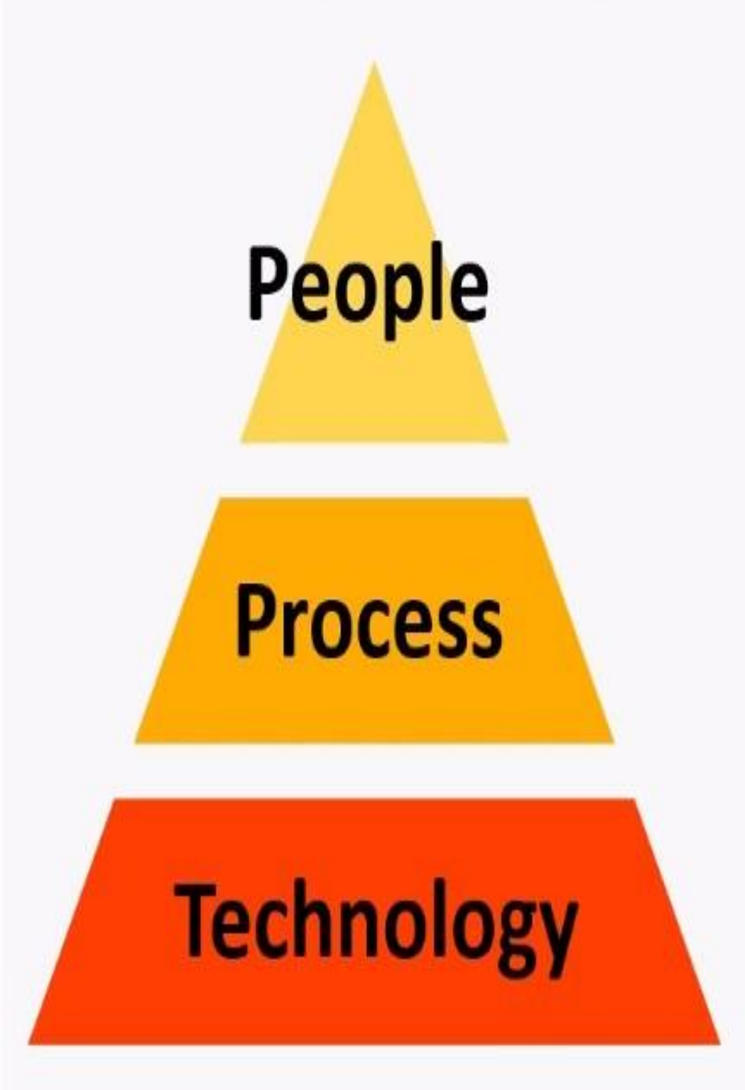
Elemen Keamanan Informasi

SNI ISO/IEC 27001:2022

Sistem Manajemen Keamanan Informasi (SMKI)



Elemen Keamanan Informasi

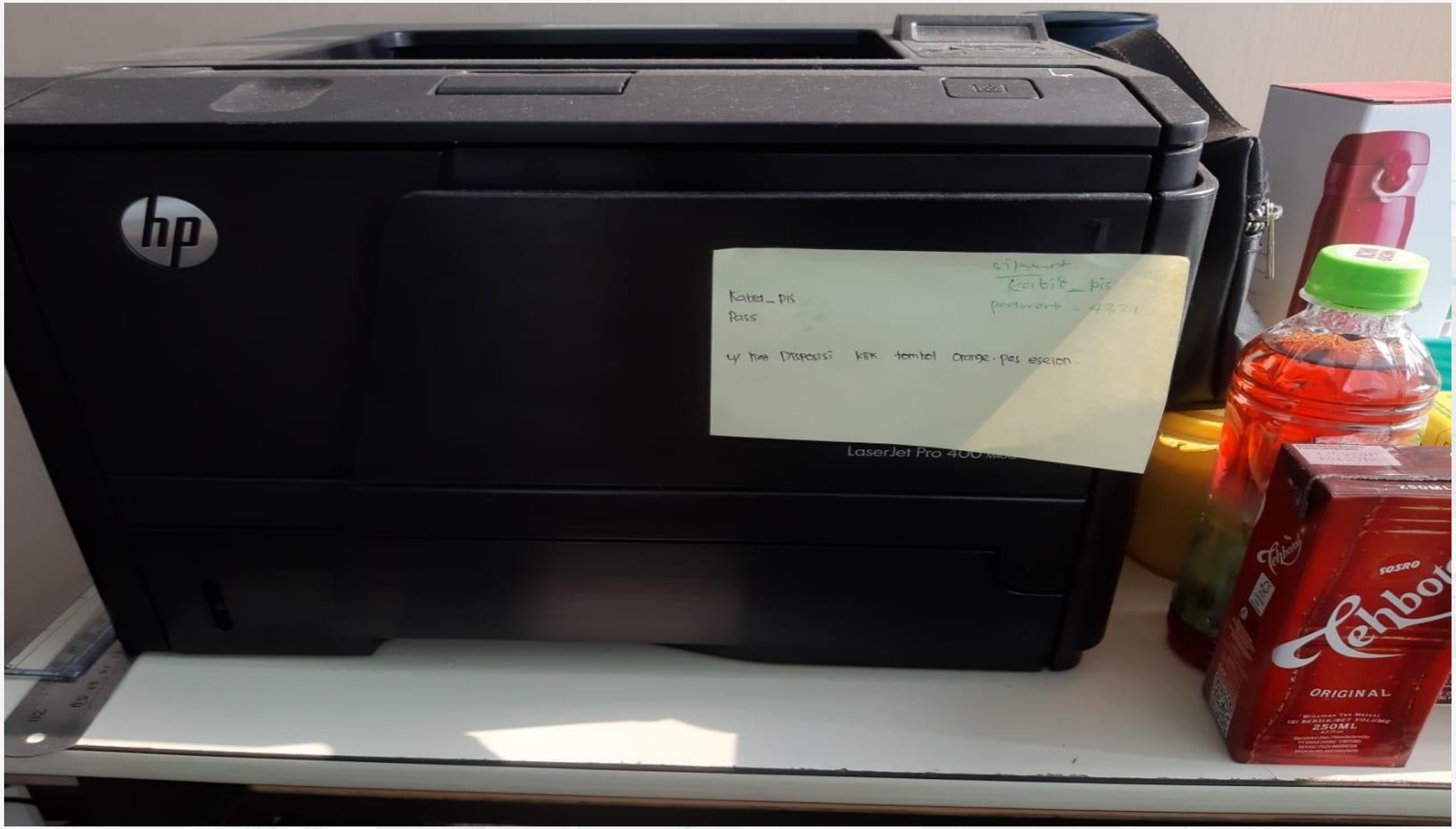


Stakeholders, Pemilik Organisasi, Pihak Manajemen, Staff / Pegawai, Vendor, Mitra Kerja, Penyedia Jasa Layanan, Konsultan, dll.

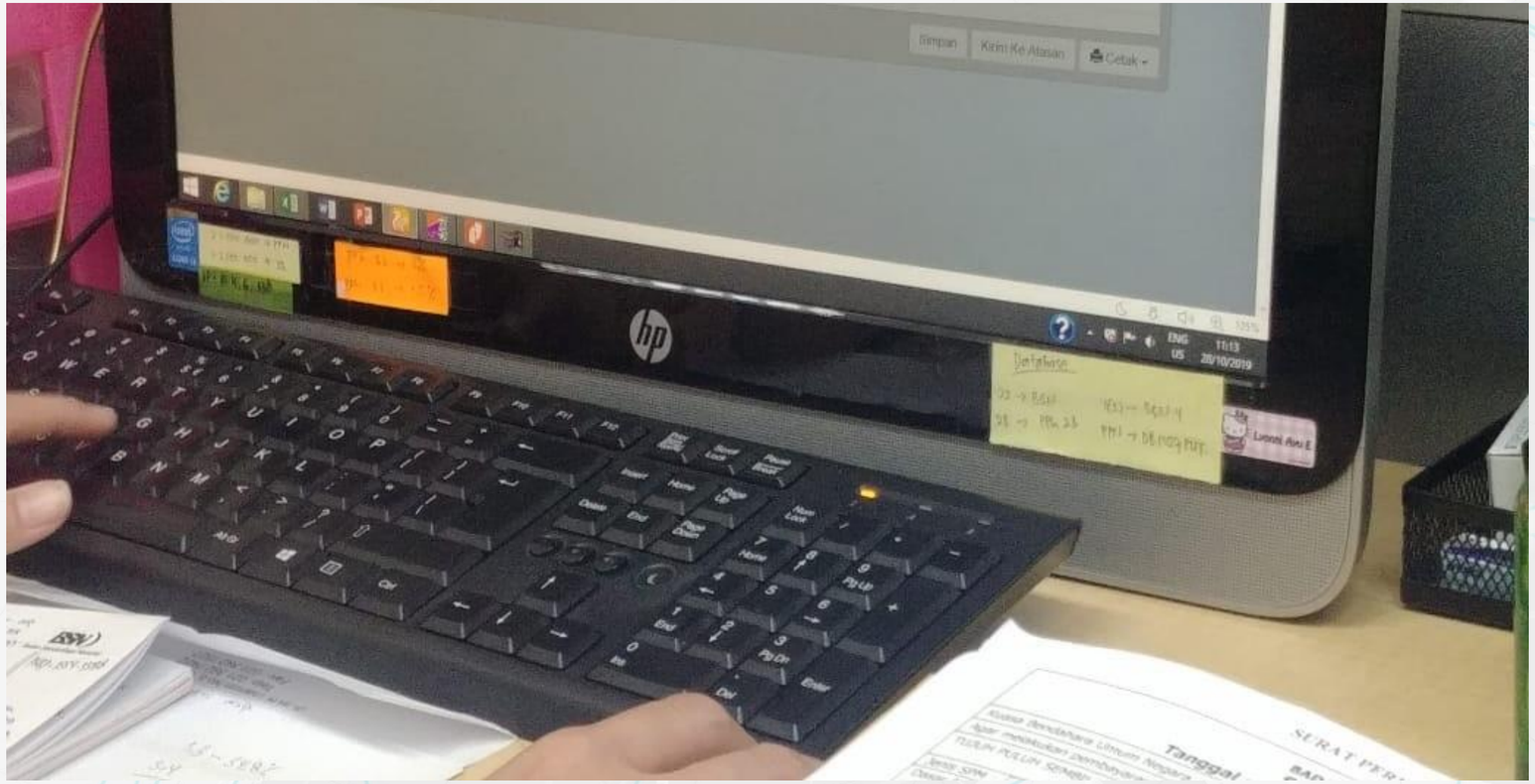
Help Desk, Pelaporan Insiden, Pemenuhan Permintaan (*Request*), Pengelolaan Akses, Pengelolaan Identitas, Pengadaan TIK, dll.

Kabel, Perangkat dan Jaringan Data/Voice, Layanan Telekomunikasi (Video Conferencing), Server, Desktop & Media Penyimpanan, Sistem Operasi, Aplikasi, dll.

User Tidak Aware SMKI

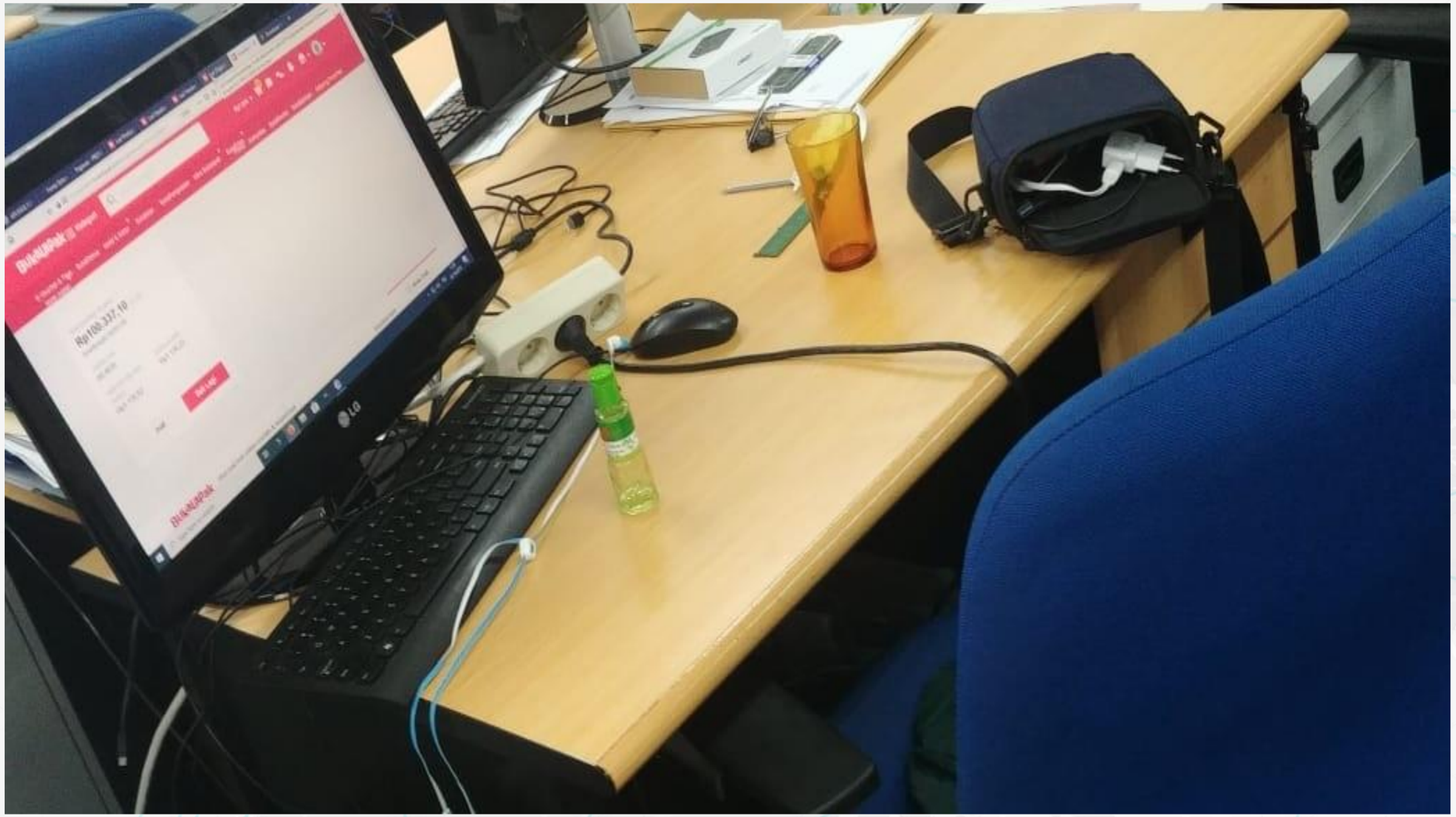


User Tidak Aware SMKI



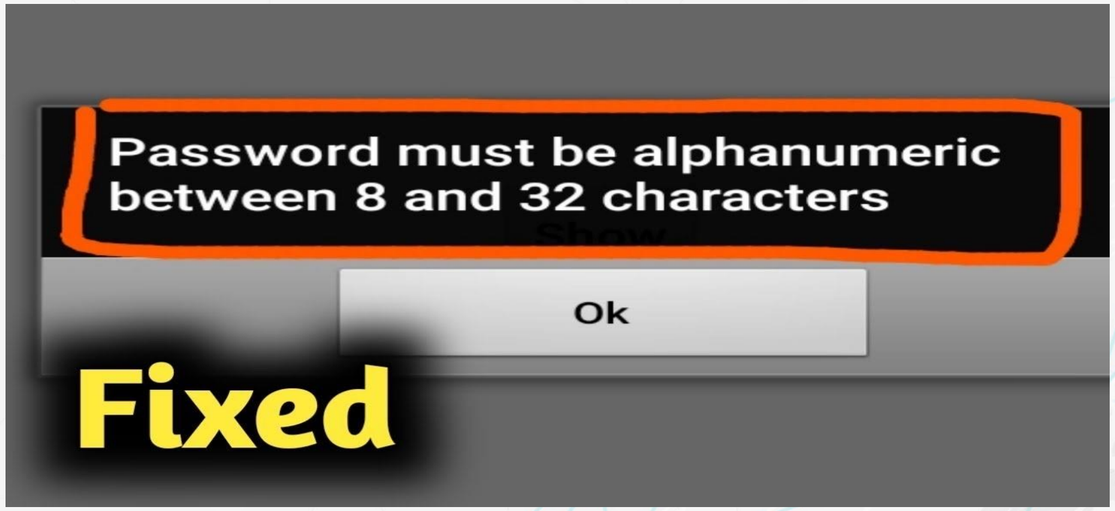
User Tidak Aware SMKI

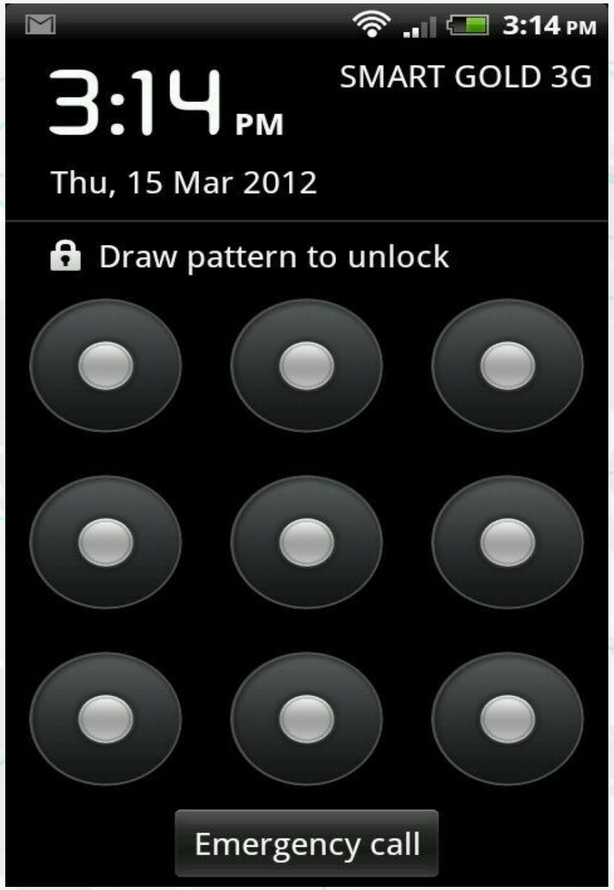
User Tidak Aware SMKI



Video Awareness

Bentuk Pengamanan SMKI



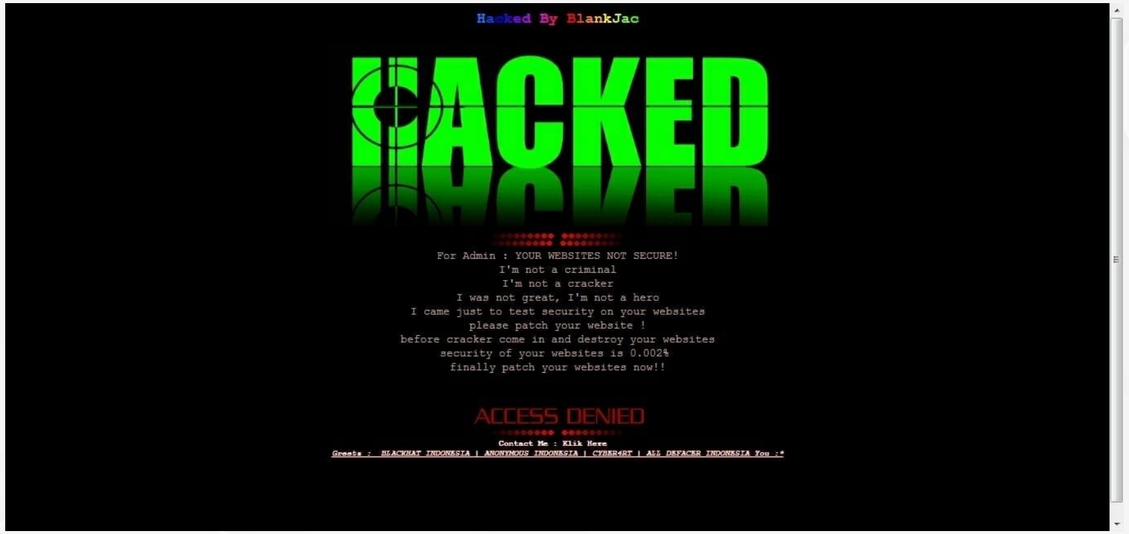


Bentuk Pengamanan SMKI

Bentuk Pengamanan SMKI

Serangan Keamanan Informasi

- Malicious Ware (Virus, Worm, Spyware, Keylogger, DOS, DDOS, etc)
- Spam, Phising
- Web Deface
- Data Leakage/Theft
- Pencurian



Motivasi Dibalik Serangan Cyber

Hanya untuk bersenang-senang

Ketenaran dan popularitas

Kegiatan yang menantang

Keuntungan finansial pribadi

Kecemburuan, kemarahan

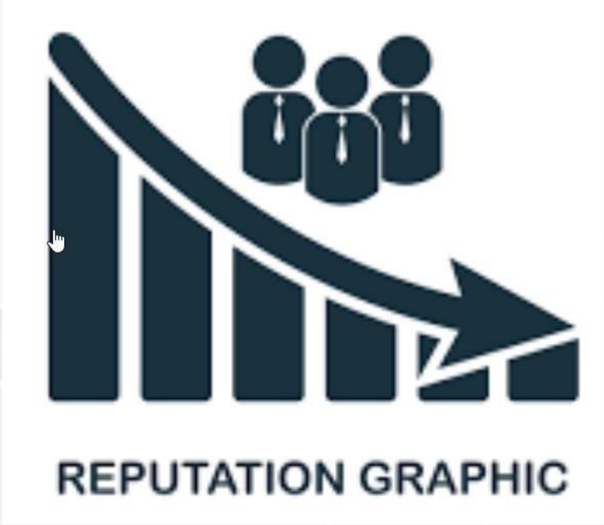
Balas dendam

Serangan acak

Ideologis / politis

Dampak Risiko

Reputasi



Finansial

Operasional

Apa itu Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) adalah pendekatan sistematis untuk mengelola informasi perusahaan yang sensitif sehingga tetap aman. Ini termasuk orang, proses dan sistem TI (Teknologi Informasi) dengan menerapkan proses manajemen risiko.

Wajib merujuk terhadap standar nasional maupun internasional yang terdapat supaya mutu pengamanan yang diberikan semakin tinggi bisa mengatasi ketika terdapat masalah

ISO

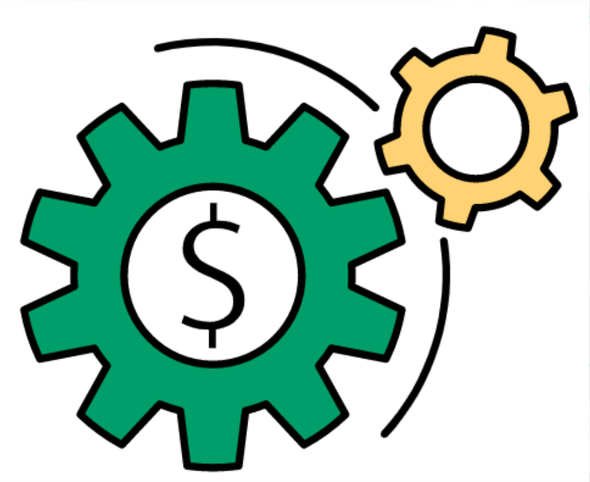
The International Standard of Organization

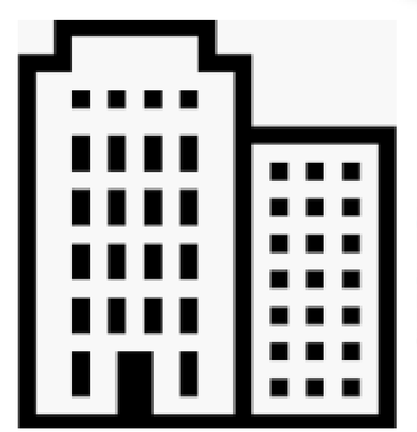
- Badan penetapan standar internasional yang terdiri dari perwakilan berbagai badan standarisasi nasional tiap negara.
- Kegiatan pokok ISO adalah menghasilkan kesepakatan-kesepakatan internasional yang kemudian dipublikasikan sebagai standar internasional.
- Contoh penerapan ISO: ukuran kartu telepon, kartu ATM Bank, ukuran dan ketebalan kertas dan lainnya

Apa itu SNI ISO/IEC 27001:2022

- Adalah satu-satunya sistem manajemen keamanan informasi (SMKI) yang berstandar internasional.
- *Auditable.*
- Mengadopsi pendekatan **P-D-C-A**.
- Berbasis Analisis Risiko dengan 93 control (pengendalian) yang harus diimplementasikan.
- Kompatibel dengan Sistem Manajemen keluaran ISO, ISO/IEC, ISO/TS, OHSAS, BS/PAS, TL.
- Komposisi: 40% Keamanan IT, 20% Keamanan Fisik, 10% Continuity, 30% Management System

Siapa Yang membutuhkan ? SNI ISO/IEC 27001:2022





Manfaat menerapkan SMKI

- Mengidentifikasi tujuan keamanan informasi
- Melindungi sumberdaya informasi dari gangguan keamanan informasi
- Mempelajari tentang tanggungjawab personil untuk menjaga keamanan informasi
- Merespon insiden keamanan informasi apabila mengalami masalah keamanan informasi.

SNI ISO/IEC 27001:2022

Logo Dokumen SNI

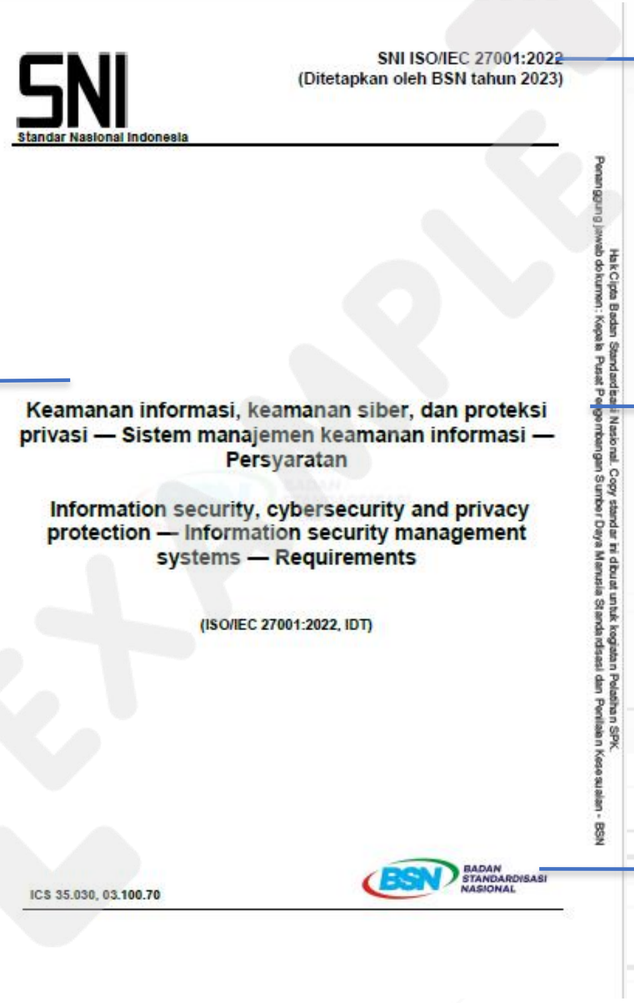
Nomor SNI

Judul SNI

Watermark

Kode International Classification Standards

Logo BSN



SNI

Standar Nasional Indonesia

SNI ISO/IEC 27001:2022
(Ditetapkan oleh BSN tahun 2023)

Keamanan informasi, keamanan siber, dan proteksi privasi — Sistem manajemen keamanan informasi — Persyaratan

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

(ISO/IEC 27001:2022, IDT)

ICS 35.030, 03.100.70

BSN BADAN STANDARDISASI NASIONAL

Hak Cipta Badan Standardisasi Nasional. Copy standar ini dibuat untuk keperluan Pelatihan SPK.
Penanggung jawab dokumen : Kepala Pusat Pengembangan Sumber Daya Manusia Standardisasi dan Penilaian Kesesuaian - BSN

Standarisasi Sistem Manajemen Keamanan Informasi

- BS 7799:1, dikenal sebagai ISO/IEC 17799 setelah diadopsi oleh ISO, disebut sebagai Information Technology Code of Practice for Information Security Management. Topik dalam ISO 17799 meliputi definisi istilah keamanan informasi, mengklasifikasi jenis informasi, menguraikan persyaratan minimum, dan menyarankan respon yang sesuai untuk pelanggaran keamanan.
- BS 7799:2 disebut sebagai Information Security Management: Specification with Guidance for Use.
- General Accepted System Security Principles atau "GASSP", yang merupakan bagian dari kumpulan penerapan sistem keamanan informasi.
- Guidelines for the Management of IT Security, atau GMITS / ISO-13335, yang menyediakan sebuah konsep kerangka kerja (framework) untuk manajemen keamanan IT.

Keluarga

ISO/IEC 27001:2022

Standard
ISO/IEC **27000**:2018
Information technology — Security techniques — Information security management systems — Overview and vocabulary

Standard
ISO/IEC **27001**:2022
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Standard
ISO/IEC **27002**:2022
Information security, cybersecurity and privacy protection — Information security controls

Standard
ISO/IEC 27003:2017
Information technology — Security techniques — Information security management systems — Guidance
ISO/IEC 27003:2017 provides explanation and guidance on ISO/IEC **27001**:2013.

Standard
ISO/IEC 27004:2016
Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

Standard
ISO/IEC 27005:2022
Information security, cybersecurity and privacy protection — Guidance on managing information security risks

Standard
ISO/IEC **27006**-1:2024
Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General

Standard
ISO/IEC **27007**:2020
Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

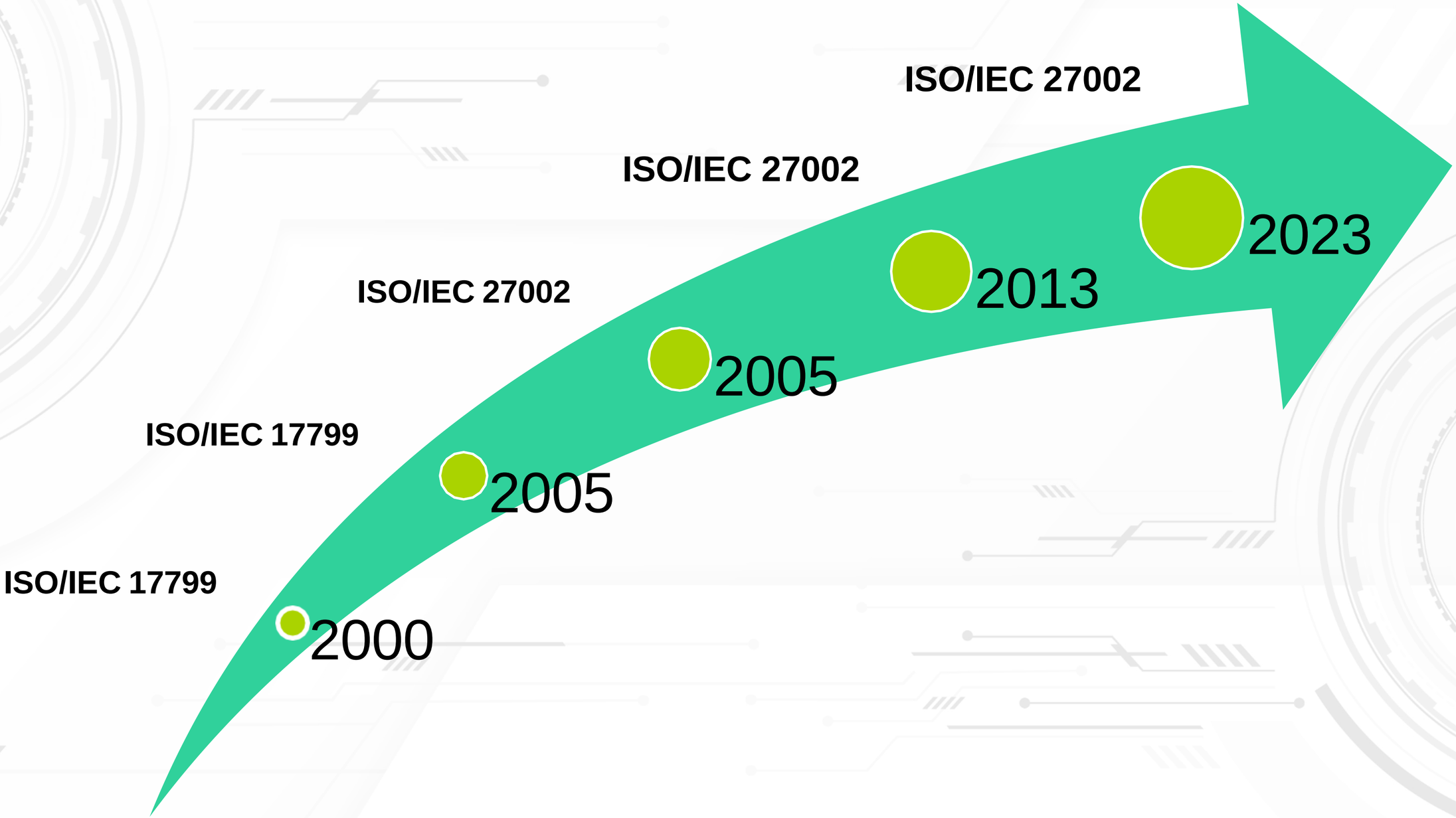
Standard
ISO/IEC TS **27008**:2019
Information technology — Security techniques — Guidelines for the assessment of information security controls

Standard
ISO/IEC 27013:2021
Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC **27001** and ISO/IEC 20000-1

Standard
ISO/IEC **27014**:2020
Information security, cybersecurity and privacy protection — Governance of information security

Sumber: www.iso.org

SNI ISO/IEC 27002:2023 ?



Perubahan Judul

versi lama → versi baru

versi lama	versi baru
SNI ISO/IEC 27001:2013 – Sistem manajemen keamanan informasi – Persyaratan (ISO/IEC 27001:2013, IDT)	SNI ISO/IEC 27001:2022 Keamanan informasi, keamanan siber, dan proteksi privasi - Sistem manajemen keamanan informasi - Persyaratan (ISO/IEC 27001:2022, IDT)

Perubahan Utama
SNI ISO/IEC 27001:2022

Judul:
Info Sec, Cybersec and Privacy Protection

Jumlah kontrol Annex A berkurang dari 114 menjadi 93

93 kontrol di restrukturisasi dari 14 menjadi 4 kategori

11 kontrol baru di Annex A

Klausul 4-10 update minor

Struktur SNI ISO/ISO 27001:2022

Klausul : Ketentuan (7)

Annex : Titik Kendali, Titik Kritis, Persyaratan (93)

4 Konteks Organisasi

5 Kepemimpinan

6 Perencanaan

7 Dukungan

93 Annex

8 Operasional

9 Evaluasi Kinerja

10 Peningkatan

Struktur SNI ISO/IEC 27001:2022

1. Ruang lingkup

2. Acuan normative

3. Istilah dan definisi

4. Konteks organisasi

1. Memahami organisasi dan komteksnya

4.2 Memahami kebutuhan dan ekspetasi dari pihak yang berkepentingan

3. Menentukan ruang lingkup SMKI
4. Sistem manajemen keamanan informasi

5. Kepemimpinan

1. Kepemimpinan dan komitmen
2. Kebijakan
3. Peran, tanggung jawab dan wewenang organisasional

6. Perencanaan

1. Tindakan untuk menangani risiko dan peluang

6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

6.3 Perencanaan perubahan

7. Dukungan

1. Sumber daya
2. Kompetensi
3. Kesadaran
4. Komunikasi
5. Informasi terdokumentasi

8. Operasi

1. Perencanaan dan pengontrolan operasional
2. Asesmen risiko keamanan informasi
3. Penanganan risiko keamanan informasi

9. Evaluasi kinerja

1. Pemonitoran, pengukuran, analisis dan evaluasi
2. Audit internal
3. Reviu manajemen

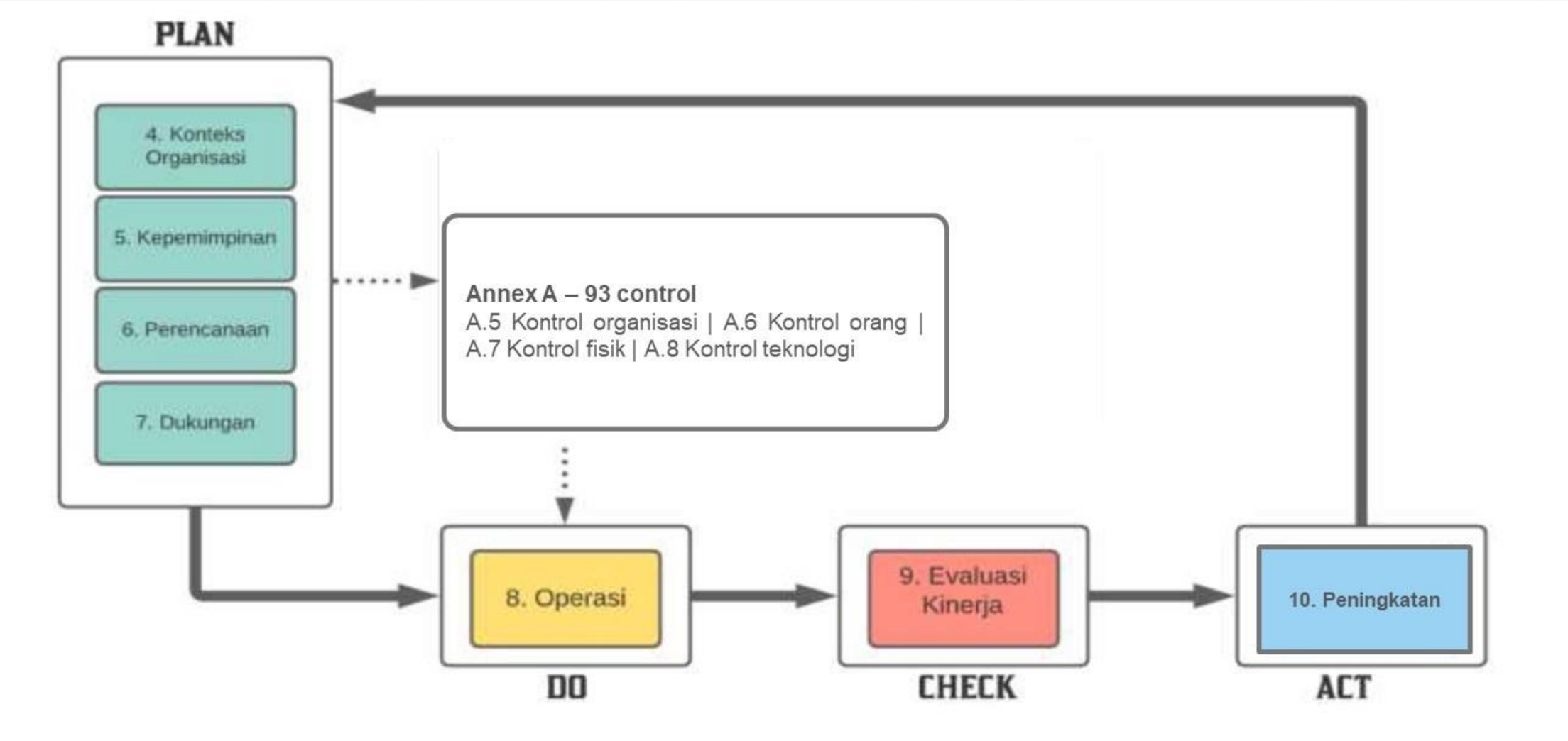
10. Peningkatan

1. Peningkatan berkelanjutan
2. Ketidaksesuaian dan Tindakan korektif

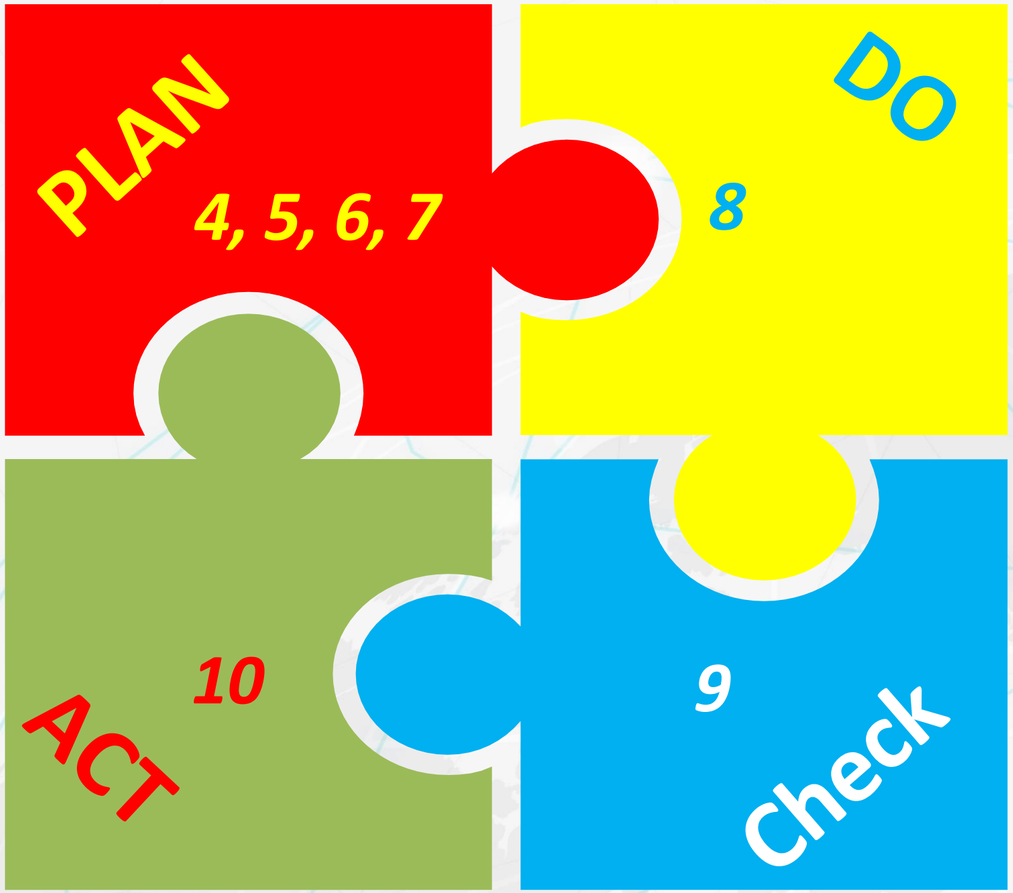
Lampiran A (normatif)

11 kontrol baru di versi 2022

Siklus PDCA SNI ISO/IEC 27001:2022



Siklus PDCA SNI ISO/ISO 27001:2022



Continual Improvement

Lampiran Annex SNI ISO/IEC 27001:2022

5. Kontrol Organisasi

5.1 Kebijakan keamanan informasi
5.2 Peran dan tanggung jawab keamanan informasi
5.3 Segregasi tugas
5.4 Tanggung jawab manajemen
5.5 Kontak dengan otoritas
5.6 Kontak dengan kelompok kepentingan khusus
5.7 Intelijen ancaman
5.8 Keamanan informasi dalam manajemen proyek
5.9 Inventarisasi informasi dan aset terkait lainnya
5.10 Penggunaan yang akseptabel dari informasi dan aset terkait lainnya
5.11 Pengembalian aset
5.12 Klasifikasi informasi
5.13 Pelabelan informasi
5.14 Transfer informasi
5.15 Kontrol akses
5.16 Manajemen identitas
5.17 Informasi autentikasi
5.18 Hak akses
5.19 Keamanan informasi dalam hubungan pemasok
5.20 Menangani keamanan informasi dalam perjanjian pemasok
5.21 Memanajemeni keamanan informasi dalam rantai pasokan TIK
5.22 Pemonitoran, reviu, dan manajemen perubahan layanan pemasok
5.23 Keamanan informasi untuk penggunaan layanan cloud
5.24 Perencanaan dan persiapan manajemen insiden keamanan informasi
5.25 Asesmen dan keputusan tentang peristiwa keamanan informasi
5.26 Respons terhadap insiden keamanan informasi
5.27 Belajar dari insiden keamanan informasi
5.28 Pengumpulan bukti
5.29 Keamanan informasi selama disrupsi
5.30 Kesiapan TIK untuk kontinuitas bisnis
5.31 Persyaratan legal, statutori, regulatori, dan kontraktual
5.32 Hak kekayaan intelektual
5.33 Proteksi rekaman
5.34 Privasi dan proteksi personal identifiable information (PII)
5.35 Reviu independen terhadap keamanan informasi
5.36 Kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi
5.37 Prosedur operasi terdokumentasi

6. Kontrol Orang

6.1 Skrining
6.2 Syarat dan ketentuan ketenagakerjaan
6.3 Kesadaran, pendidikan dan pelatihan keamanan informasi
6.4 Proses kedisiplinan
6.5 Tanggung jawab setelah terminasi atau perubahan pekerjaan
6.6 Perjanjian konfidensialitas atau nirungkap
6.7 Telekarya (Remote working)
6.8 Pelaporan peristiwa keamanan informasi

7. Kontrol Fisik

7.1 Perimeter keamanan fisik
7.2 Entri fisik
7.3 Mengamankan kantor, ruangan, dan fasilitas
7.4 Pemonitoran keamanan fisik
7.5 Memproteksi dari ancaman fisik dan lingkungan
7.6 Bekerja di area yang aman
7.7 Meja bersih dan layar bersih
7.8 Penempatan dan proteksi peralatan
7.9 Keamanan aset di luar lokasi
7.10 Media penyimpanan
7.11 Utilitas pendukung
7.12 Keamanan perkabelan
7.13 Pemeliharaan peralatan
7.14 Pemusnahan atau penggunaan kembali peralatan dengan aman

8. Kontrol Teknologi

8.1 Perangkat titik akhir pengguna
8.2 Hak akses privilese
8.3 Pembatasan akses informasi
8.4 Akses ke kode sumber
8.5 Autentikasi aman
8.6 Manajemen kapasitas
8.7 Proteksi terhadap perangkat perusak
8.8 Manajemen kerentanan teknis
8.9 Manajemen konfigurasi
8.10 Penghapusan informasi
8.11 Penyamaran (masking) data
8.12 Pencegahan kebocoran data
8.13 Pencadangan informasi
8.14 Redundansi fasilitas pemrosesan informasi
8.15 Membuat log
8.16 Pemonitoran aktivitas
8.17 Sinkronisasi jam
8.18 Penggunaan program utilitas privilese
8.19 Instalasi perangkat lunak pada sistem operasional
8.20 Keamanan jaringan
8.21 Keamanan layanan jaringan
8.22 Segregasi jaringan
8.23 Pemfilteran web
8.24 Penggunaan kriptografi
8.25 Siklus hidup pengembangan yang aman
8.26 Persyaratan keamanan aplikasi
8.27 Prinsip-prinsip arsitektur dan rekayasa sistem yang aman
8.28 Pengkodean yang aman
8.29 Pengujian keamanan dalam pengembangan dan penerimaan
8.30 Pengembangan yang dialihdayakan
8.31 Pemisahan lingkungan pengembangan, pengujian, dan produksi
8.32 Manajemen perubahan
8.33 Informasi uji
8.34 Proteksi sistem informasi selama pengujian audit

Statement of Applicability (SOA)

Dokumentasi Analisis Kontrol Implementasi SMKI

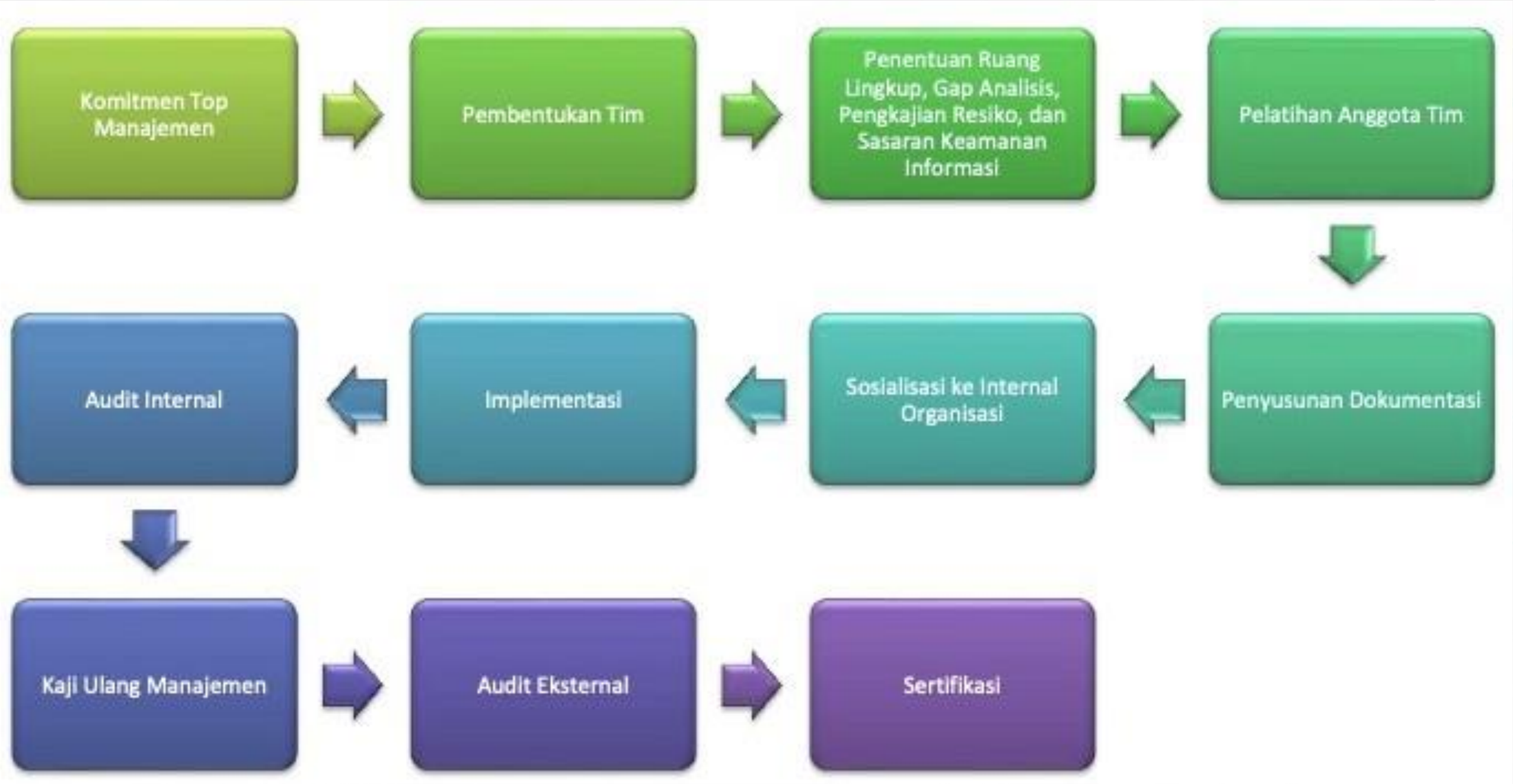
Pernyataan Kontrol terhadap Annex A SNI ISO/IEC 27001:2022

4 Domain dan 93 Kontrol Keamanan Informasi

Statement of Applicability (SOA)

Versi	1.0						
Tanggal	27 MEI 2024						
Ruang Lingkup SMKI	Sistem Informasi Audit Keuangan ABC						
ISO/IEC 27001:2022 Statement of Applicability				**Apakah kontrol bisa diaplikasikan? (YA / TIDAK)**	**Alasan / Keterangan pemilihan kendali annex**	**Referensi dokumen/bukti dukung (Kebijakan, prosedur, formulir)**	**Keterangan Tambahan (jika Ada)**
Section	**Control**		**Deskripsi Kontrol**				
			A.5. Organizational controls				
A.5.1	Policies for information security		Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	YA	Diterapkan keseluruhan di Organisasi	Pedoman SMKI Ver 1.2	
A.5.2	Information security roles and responsibilities		Information security roles and responsibilities shall be defined and allocated according to the organization needs.	YA	Diterapkan keseluruhan di Organisasi	Pedoman SMKI Ver 1.2	
A.5.3	Segregation of duties		Conflicting duties and conflicting areas of responsibility shall be segregated.	YA	Diterapkan keseluruhan di Organisasi	Pedoman SMKI Ver 1.2	
A.5.4	Management responsibilities		Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	YA	Diterapkan keseluruhan di Organisasi	Pedoman SMKI Ver 1.2	
A.5.5	Contact with authorities		The organization shall establish and maintain contact with relevant authorities.	YA	Diterapkan keseluruhan di Organisasi	Pedoman SMKI Ver 1.2	

Sekilas Tahapan Implementasi SMKI



Contoh Sertifikat SNI ISO/IEC 27001:2022

CERTIFICATE

SUCOFINDO

Certificate No.

SUCOFINDO INTERNATIONAL CERTIFICATION SERVICES

Graha Sucofindo B1 Floor - Jl. Raya Pasar Minggu Kav. 34 Jakarta 12780
Phone : +62-21-7983666 ext. 1021; Fax : +62-21-7987015 / 7987029; Email : cs.sics@sucofindo.co.id

Menyatakan bahwa
Certify that

(Nama Instansi/Lembaga/Organisasi)

(Alamat Instansi/Lembaga/Organisasi)

telah menerapkan sistem manajemen keamanan informasi yang memenuhi
has implemented information security management system that comply with

SNI ISO/IEC 27001:2013
Information Security Management Systems-Requirements
Persyaratan-Sistem Manajemen Keamanan Informasi

Ruang lingkup sertifikasi :
The scope of certification :

Sistem Manajemen Keamanan Informasi pada Pusat Data dan Sistem Informasi.

Statement of Applicability Ver 1.0 date. 16 Juli 2019

Kebijakan Transisi Sertifikasi 27001 (IAF MD Issue 2)

Activity	Due Date
AB	
AB to be ready to assess to ISO/IEC 27001:2022 no later than	6 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 30 April 2023)
Initial assessment by AB to ISO/IEC 27001:2022 only, to begin no later than	6 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 30 April 2023)
AB transitions of CABs completed by	12 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 31 October 2023)
CAB	
Initial certification and recertification by CAB to ISO/IEC 27001:2022 only, to begin no later than	18 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 30 April 2024)
CAB transitions of certified clients completed by	36 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 31 October 2025)

KAN telah mengadopsi menjadi kebijakan KAN No. 011/KAN/11/2023

Keuntungan menerapkan SNI ISO/IEC 27001:2022

- ✓ Membuat pengaruh positif dalam hal citra perusahaan, nilai, dan persepsi yang baik dari pihak lain.
- ✓ Memastikan bahwa organisasi memiliki kontrol terkait keamanan informasi terhadap lingkungan proses bisnisnya yang mungkin menimbulkan risiko atau gangguan.
- ✓ Dapat digabung atau dikombinasikan dengan sistem manajemen lainnya seperti SNI ISO 9001, SNI ISO 14000, SNI ISO 20000, SNI ISO 37001, SNI ISO 38500, ITIL, COBIT dll.
- ✓ Salah satu standar pengamanan informasi yang diakui di seluruh dunia.
- ✓ Patuh terhadap hukum dan undang-undang seperti UU ITE, dll.
- ✓ Meningkatkan awareness terhadap keamanan informasi pada pegawai/karyawan.

Tantangan menerapkan SNI ISO/IEC 27001:2022

- ✓ Komitmen dan Dukungan Pimpinan
- ✓ SDM yang dimiliki organisasi
- ✓ Berubah adalah hal yang sulit
- ✓ Teknologi;

Tipe Planning

- ***Incident Response Planning*** **(IRP),** terdiri dari satu set proses dan prosedur detil yang mengantisipasi, mendeteksi, dan mengurangi akibat dari insiden yang tidak diinginkan yang membahayakan sumberdaya informasi dan aset organisasi.
- ***Disaster Recovery Planning*** **(DRP)**, persiapan jika terjadi bencana, dan melakukan pemulihan dari bencana.
- ***Business Continuity Planning*** **(BCP)**, menjamin bahwa fungsi kritis organisasi tetap bisa berjalan jika terjadi bencana. Jika terjadi bencana, BCP bertugas menjamin kelangsungan fungsi kritis di tempat alternatif. Faktor penting yang diperhitungkan dalam BCP adalah biaya.

Protection

Proteksi dilaksanakan melalui serangkaian aktifitas manajemen resiko, meliputi perkiraan resiko (risk assessment) dan pengendali, termasuk mekanisme proteksi, teknologi proteksi dan perangkat proteksi baik perangkat keras maupun perangkat keras. Setiap mekanisme merupakan aplikasi dari aspek-aspek dalam rencana keamanan informasi.

People

penghubung utama dalam program keamanan informasi. Penting sekali mengenali aturan krusial yang dilakukan oleh pekerja dalam program keamanan informasi. Aspek ini meliputi personil keamanan dan keamanan personil dalam organisasi.

Evaluasi

Jelaskan manfaat dan tujuan penggunaan ISO27001 pada perusahaan/organisasi.

SISTEM MANAJEMEN KEAMANAN INFORMASI SNI ISO/IEC 27001:2022

Materi 2 - Klausul 4 Konteks Organisasi

SNI ISO/IEC 27001:2022

1. Ruang lingkup

2. Acuan normative

3. Istilah dan definisi

4. Konteks organisasi

4.1 Memahami organisasi dan komteksnya

4.2 Memahami kebutuhan dan ekspetasi dari pihak yang berkepentingan

4.3 Menentukan ruang lingkup SMKI

4.4 Sistem manajemen keamanan informasi

5. Kepemimpinan

5.1 Kepemimpinan dan komitmen

5.2 Kebijakan

5.3 Peran, tanggung jawab dan wewenang organisasional

6. Perencanaan

6.1 Tindakan untuk menangani risiko dan peluang

6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

6.3 Perencanaan perubahan

7. Dukungan

7.1 Sumber daya

7.2 Kompetensi

7.3 Kesadaran

7.4 Komunikasi

7.5 Informasi terdokumentasi

8. Operasi

8.1 Perencanaan dan pengontrolan operasional

8.2 Asesmen risiko keamanan informasi

8.3 Penanganan risiko keamanan informasi

9. Evaluasi kinerja

9.1 Pemonitoran, pengukuran, analisis dan evaluasi

9.2 Audit internal

9.3 Reviu manajemen

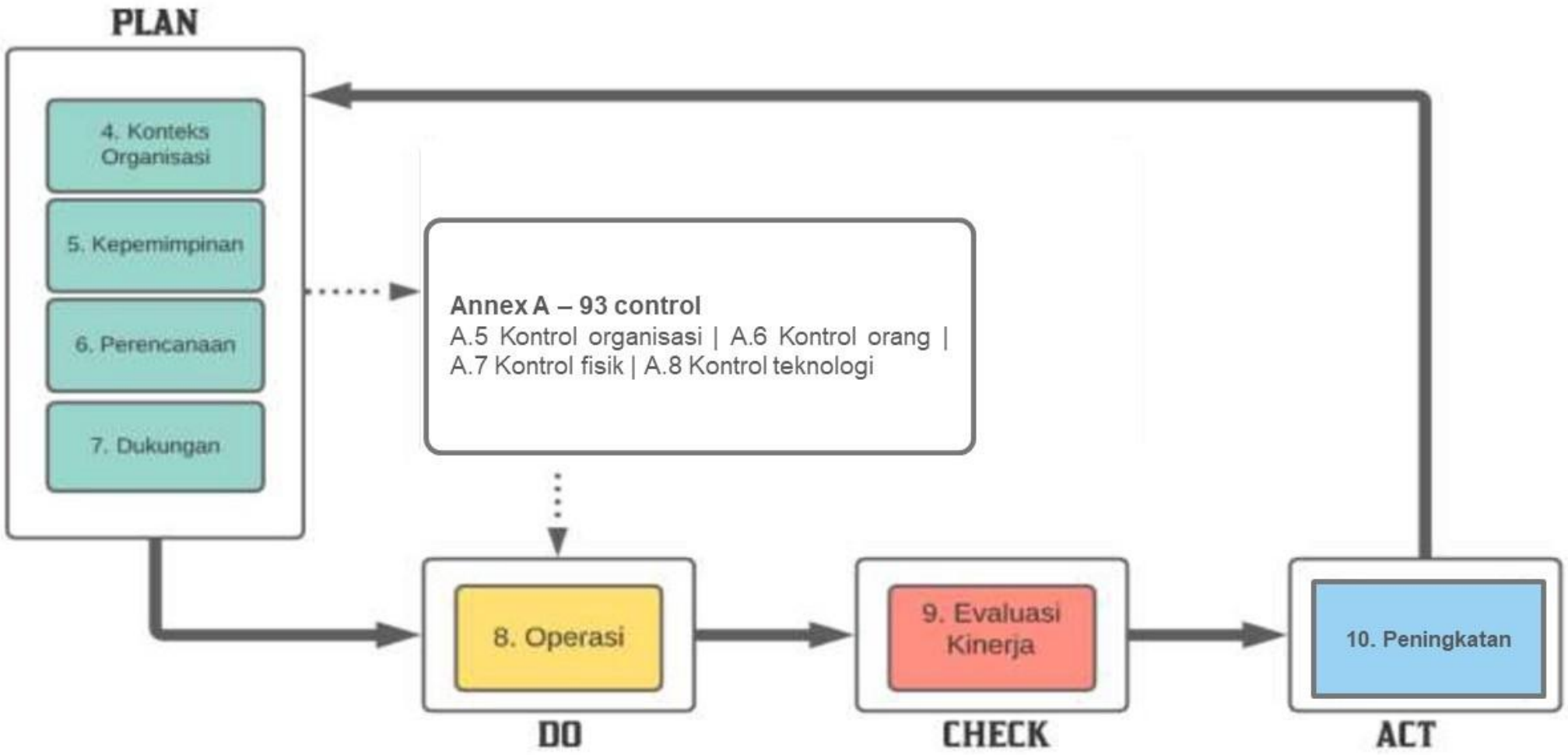
10. Peningkatan

10.1 Peningkatan berkelanjutan

10.2 Ketidaksesuaian dan Tindakan korektif

Lampiran A (normatif)

Siklus PDCA SNI ISO/IEC 27001:2022



Perubahan Minor Klausul 4

4.2 Memahami kebutuhan dan harapan dari pihak yang bekepentingan Organisasi harus menentukan: pihak yang berkepentingan yang relevan dengan SMKI; dan persyaratan pihak yang berkepentingan ini yang terkait dengan keamanan informasi. **CATATAN** Persyaratan pihak yang berkepentingan dapat mencakup persyaratan hukum dan peraturan perundang undangan, serta kewajiban kontraktual.	**4.2. Memahami kebutuhan dan harapan pihak yang berkepentingan** Organisasi harus menentukan: a) pihak berkepentingan yang relevan dengan sistem manajemen keamanan informasi; b) persyaratan yang relevan dari pihak yang berkepentingan ini; c) persyaratan mana yang akan dipenuhi melalui sistem manajemen keamanan informasi. ***CATATAN*** Persyaratan pihak berkepentingan dapat mencakup persyaratan hukum dan peraturan dan kewajiban kontraktual.

4.1

Add the following sentence at the end of the subclause:

The organization shall determine whether climate change is a relevant issue.

4.2

Add the following note at the end of the subclause:

NOTE 2 Relevant interested parties can have requirements related to climate change.

Published
ISO/IEC 27001:2022/Amd 1:2024
Stage: **60.60**

Klausul 4.1 Memahami Organisasi dan Konteksnya

- Organisasi harus menentukan isu eksternal dan internal yang relevan dengan tujuannya dan yang mempengaruhi kemampuannya untuk mencapai manfaat yang diharapkan dari sistem manajemen keamanan informasi organisasi.

Catatan:

- Penentuan isu ini mengacu ke penetapan konteks eksternal dan internal dari organisasi yang dipertimbangkan dalam Pasal 5.4.1 dari ISO 31000:2018.
- Isu Eksternal dan Internal harus dikaji ulang dan dimonitor

Klausul 4.1 Memahami Organisasi dan Konteksnya

Contoh identifikasi permasalahan / isu internal dan eksternal:

- Organisasi XYZ ingin melakukan sertifikasi SNI ISO/IEC 27001, password default karyawan tidak diubah (isu internal);
- ada Peraturan Menteri Kominfo bahwa penyelenggara pelayanan publik secara elektronik harus menerapkan dan atau sertifikasi SNI ISO/IEC 27001 (isu Eksternal)

Klausul 4.1 Memahami Organisasi dan Konteksnya

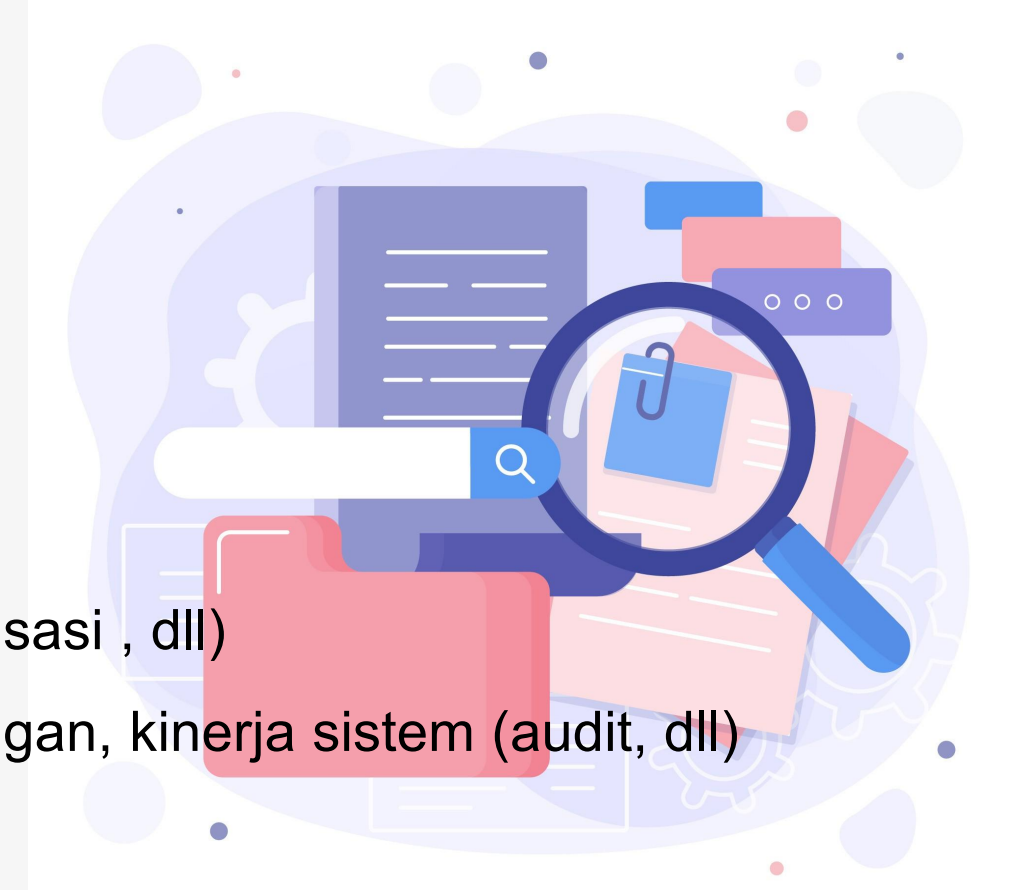
Sumber isu eksternal dan isu internal bisa berasal dari kajian-kajian dokumen-dokumen organisasi seperti:

- Hasil rapat internal
- Kajian dokumen internal
- Publikasi ekternal
- Hasil rapat dengan stakeholder
- Hasil audit internal dan eksternal
- Hasil rapat Tinjauan Manajemen
- Rencana Strategis (Renstra)

Klausul 4.1 Memahami Organisasi dan Konteksnya

Contoh sumber **isu Internal**, yaitu :

- Kinerja Organisasi
- Sarana dan Prasarana
- Kondisi atau lingkungan operasional
- Knowledge organisasi terkait keamanan informasi
- Sumber Daya Manusia (kompetensi, budaya organisasi , dll)
- Aktivitas atau operasional, tingkat kepuasan pelanggan, kinerja sistem (audit, dll)
- Struktur Organisasi



Klausul 4.1 Memahami Organisasi dan Konteksnya

Contoh sumber **isu Eksternal**, yaitu : Metode **PESTLE**

- **Political/Politik** (PSBB/PPKM, Pemilu, International Agreements, Stabilitas politik, Infrastruktur lokal, dll)
- **Economic/Ekonomi** (suasana ekonomi, inflasi,dll)
- **Social** (Pandemi Covid-19, Tingkatan edukasi, Hari Libur Nasional dan hari Kerja, dll)
- **Technological/Teknologi** (Teknologi baru, material dan peralatan baru, paten, sertifikasi personel, dll)
- **Legal** (peraturan perundangan terkait teknologi informasi/keamanan informasi/sistem elektronik)
- **Environment/Lingkungan** (isu lingkungan di bidang teknologi informasi, dll)

Contoh Isu Internal dan Eksternal

ISSUE	Eksternal	Internal
Kebijakan, peraturan perundang-undangan dan rencana pembangunan nasional	Visi dan Misi Presiden Republik Indonesia, kegiatan dan sektor prioritas nasional dalam RPJPN dan RPJMN.	-
	Pandemic Covid-19	-
Kesadaran dan Kepercayaan Pemangku Kepentingan	Adanya kesepakatan perdagangan bilateral, regional, dan multilateral untuk memanfaatkan peluang pasar dan peningkatan ekspor produk Indonesia ke manca negara sehingga dibutuhkan suatu sistem manajemen keamanan informasi terkait keamanan data dan informasi	-
Ketersediaan, Kualitas dan kapasitas Sumber Daya	-	Sarana dan prasarana TI yang tersedia masih belum mampu menjamin keamanan, kerahasian, keutuhan, dan ketersediaannya yang diperlukan untuk mendukung seluruh tugas pokok dan fungsi
Budaya Organisasi	-	Proses Bisnis Sistem Manajemen Keamanan Informasi, Tata Nilai, dan Budaya Organisasi belum sepenuhnya dipahami dan diterapkan oleh personel Instansi X

Tugas Klausul 4

1. Tim Mahasiswa merancang perusahaan/organisasi beserta struktur organisasinya.
2. Mahasiswa mendefinisikan Faktor Internal dan Eksternal Organisasi masing-masing yang akan menerapkan SMKI.

Klausul 4.2 Memahami kebutuhan dan ekspektasi dari pihak yang berkepentingan

Organisasi harus menentukan:

a) pihak yang berkepentingan yang relevan dengan SMKI;

b) persyaratan yang relevan dari pihak yang berkepentingan tersebut;

c) persyaratan yang mana yang akan ditangani melalui sistem manajemen keamanan informasi.

Persyaratan pihak yang berkepentingan dapat mencakup persyaratan hukum dan peraturan perundang-undangan, serta kewajiban kontraktual.

Contoh Daftar Peraturan Perundang-undangan

No	Daftar Hukum dan Perundang-undangan
1	Undang-Undang No.8 Tahun 1999 tentang Perlindungan Konsumen
2	Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik
3	Perpres No. 95 Tahun 2018 tentang SPBE
4	-
5	-

Klausul 4.3 Menentukan ruang lingkup sistem manajemen keamanan informasi

- Organisasi harus menentukan batasan dan penerapan SMKI untuk menetapkan ruang lingkup SMKI.
- Ketika menentukan ruang lingkup ini, organisasi harus mempertimbangkan:
  a) isu eksternal dan internal seperti yang sudah dipetakan di level institusi
  b) persyaratan yang dimaksud terkait perundangan-undangan yang terkait dan perjanjian kontraktual
  c) relasi hubungan operasional dengan stakeholder.

Ruang lingkup harus tersedia sebagai informasi yang terdokumentasi.

Klausul 4.3 Menentukan ruang lingkup sistem manajemen keamanan informasi

Organisasi harus menentukan batasan dan penerapan SMKI untuk menetapkan ruang lingkup SMKI.

Ketika menentukan ruang lingkup ini, organisasi harus mempertimbangkan:

a) isu eksternal dan internal seperti yang sudah dipetakan di level institusi

b) persyaratan yang dimaksud terkait perundangan-undangan yang terkait dan perjanjian kontraktual

c) relasi hubungan operasional dengan stakeholder.

Ruang lingkup harus tersedia sebagai informasi yang terdokumentasi.

Klausul 4.3 Menentukan ruang lingkup sistem manajemen keamanan informasi

- Misalnya: Penyediaan layanan publik, Pengamanan Pusat Data, pengembangan aplikasi, penggunaan jaringan dan fasilitas email, dan sebagainya

Proses dan/atau Kegiatan

Satuan Kerja

- Misalnya: Direktorat, Departemen atau Bidang

Lokasi kerja

- Misalnya: Tingkat Pusat, daerah atau keduanya

Metode yang dapat digunakan untuk menentukan ruang lingkup

Klausul 4.4 Sistem Manajemen Keamanan Informasi

Organisasi harus *menetapkan, menerapkan, memelihara dan memperbaiki* secara berkelanjutan SMKI, termasuk proses-proses yang diperlukan dan interaksinya, berdasarkan persyaratan pada dokumen ini.

Menetapkan → **Terdapat dokumen yang ditandatangani oleh pimpinan puncak**

Menerapkan → **Terdapat dokumen yang dijadikan acuan**

Memelihara → **Terdapat kegiatan pemantauan, pengukuran dan evaluasi**

Memperbaiki → **Terdapat tindakan koreksi**

Klausul 5 - Kepemimpinan

SubKlausul 5.1
Kepemimpinan dan Komitmen

SubKlausul 5.2 Kebijakan

SubKlausul 5.3 Peran ,
Tanggung Jawab dan Wewenang
Organisasional

Istilah dan Definisi

- **Manajemen puncak** adalah orang atau sekelompok orang yang mengarahkan dan mengendalikan suatu organisasi di tingkatan tertinggi
- Manajemen puncak memiliki kekuasaan untuk mendelegasikan wewenang dan menyediakan sumber daya di dalam organisasi
- Jika ruang lingkup sistem manajemen hanya mencakup bagian dari suatu organisasi, manajemen puncak merujuk kepada mereka yang mengarahkan dan mengendalikan bagian organisasi itu
- **Kebijakan** adalah keinginan dan arahan dari suatu organisasi sebagaimana dinyatakan secara resmi oleh manajemen puncaknya

SubKlausul 5.1 - Kepemimpinan dan Komitmen

Manajemen puncak harus menunjukkan kepemimpinan dan komitmen terkait SMKI dengan cara:

a) memastikan **kebijakan** keamanan informasi dan **sasaran** keamanan informasi **ditetapkan** dan selaras dengan arah strategis organisasi;

Kebijakan

Sasaran

PM

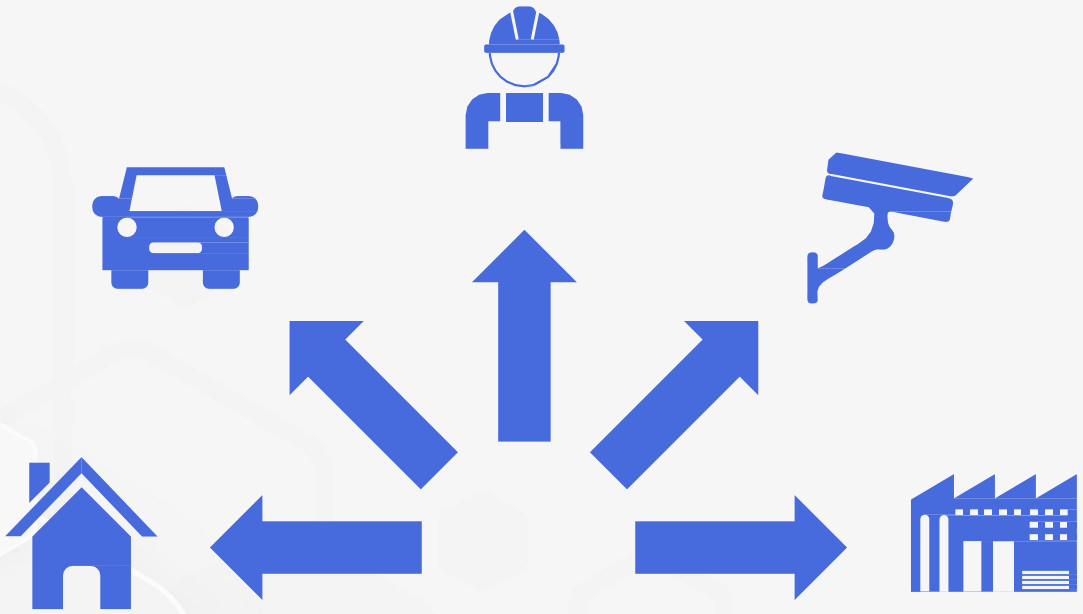
SubKlausul 5.1 - Kepemimpinan dan Komitmen

b) memastikan persyaratan SMKI terintegrasi ke dalam proses organisasi;

PM - Kepemimpinan

SubKlausul 5.1 - Kepemimpinan dan Komitmen

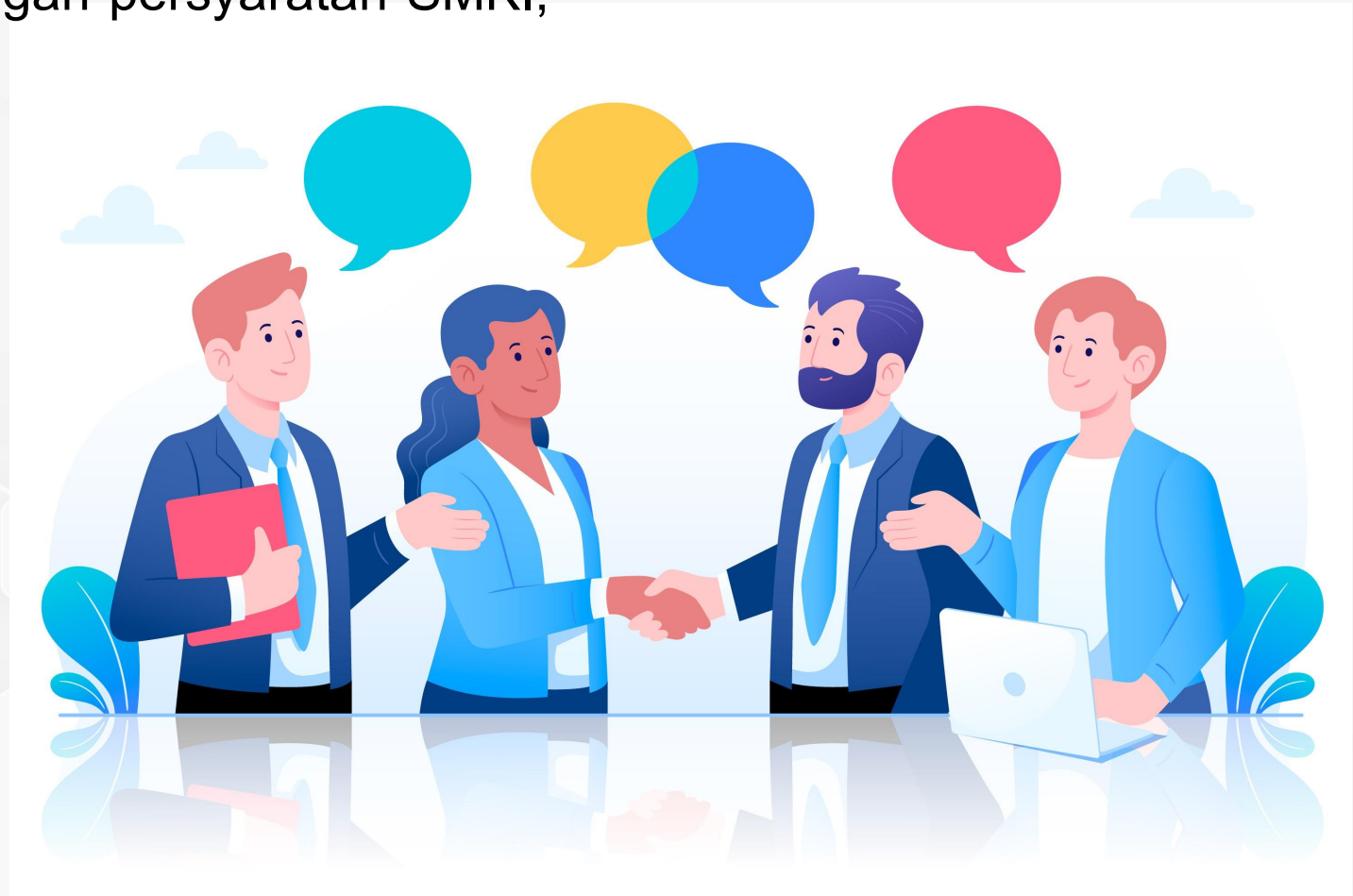
c) memastikan tersedianya sumber daya yang dibutuhkan untuk SMKI;



Klausul 7 – Dukungan

SubKlausul 5.1 - Kepemimpinan dan Komitmen

d) mengkomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan SMKI;



SubKlausul 5.1 - Kepemimpinan dan Komitmen

e) memastikan bahwa SMKI mencapai manfaat yang diharapkan;

f) memberikan arahan dan dukungan pada personel untuk berkontribusi dalam efektivitas SMKI;

g) mempromosikan perbaikan berkelanjutan; dan

h) mendukung peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.

SubKlausul 5.2 Kebijakan

Manajemen puncak **harus** menetapkan kebijakan keamanan informasi yang:

a) sesuai dengan tujuan organisasi;

b) mencakup sasaran keamanan informasi (lihat 6.2) atau menyediakan kerangka kerja untuk menetapkan sasaran keamanan informasi;

c) mencakup komitmen untuk memenuhi persyaratan yang berlaku terkait dengan keamanan informasi; dan

d) mencakup komitmen untuk perbaikan berkelanjutan terhadap SMKI.

SubKlausul 5.2 Kebijakan

Kebijakan keamanan informasi harus:

a) disediakan sebagai informasi yang terdokumentasi;

b) dikomunikasikan dalam organisasi; dan

c) disediakan untuk pihak yang berkepentingan, jika diperlukan.

- Kebijakan SMKI harus didokumentasikan
- Media dokumen ditentukan organisasi sesuai dengan kebijakan yang berlaku
- Kebijakan SMKI boleh dibuat tersendiri atau diintegrasikan dengan misalnya kebijakan mutu atau kebijakan lainnya yang berlaku di organisasi.

SubKlausul 5.3 Peran , Tanggung Jawab dan Wewenang Organisasional

Manajemen puncak harus memastikan bahwa tanggung jawab dan wewenang untuk peran yang relevan dengan keamanan informasi telah ditugaskan dan dikomunikasikan dalam organisasi.

Manajemen puncak harus menetapkan tanggung jawab dan wewenang untuk:

a) memastikan bahwa SMKI sesuai dengan persyaratan dari Standar ini;

b) melaporkan kinerja SMKI kepada manajemen puncak.

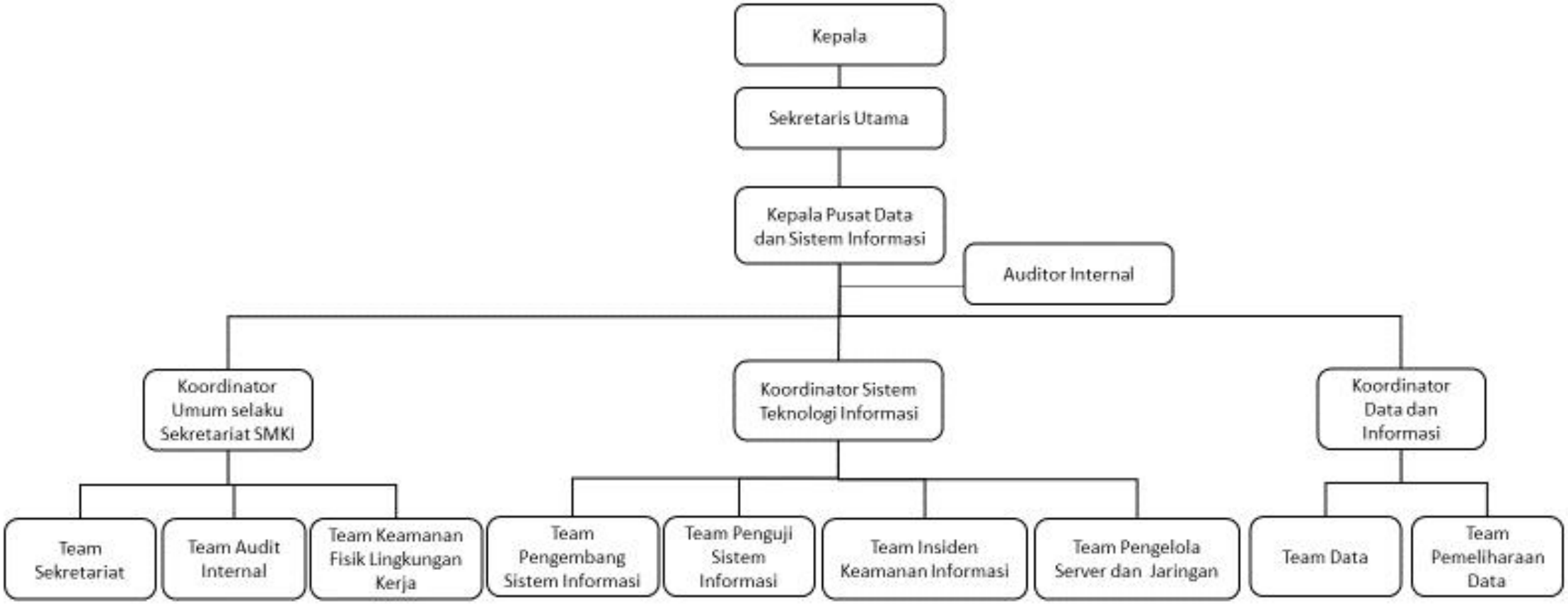
Catatan: Manajemen puncak juga dapat menetapkan tanggung jawab dan wewenang untuk melaporkan kinerja SMKI dalam organisasi.

SubKlausul 5.3 Peran , Tanggung Jawab dan Wewenang Organisasional

Manajemen puncak harus menetapkan dan mengkomunikasikan **tanggung jawab dan wewenang** keamanan informasi untuk menjamin SMKI berjalan sesuai dengan standar ISO 27001 dan melaporkan kinerja SMKI kepada manajemen puncak.

Tanggung jawab dan wewenang yang berkaitan dengan keamanan informasi perlu **ditetapkan** oleh manajemen puncak. Kegiatan ini mencakup:

- mengoordinasikan pembentukan, penerapan, pemeliharaan, pelaporan kinerja, dan peningkatan SMKI;
- melakukan koordinasi penilaian dan pemeliharaan risiko keamanan informasi;
- mengembangkan proses dan sistem keamanan informasi;
- menetapkan standar mengenai penentuan, konfigurasi dan pengoperasian kontrol keamanan keamanan informasi ;
- mengelola insiden keamanan informasi;
- melakukan kegiatan audit internal SMKI.



Contoh Struktur Organisasi Penerap SMKI

Contoh Kebijakan

Kepala Dinas XYZ berkomitmen untuk menetapkan kebijakan keamanan informasi yang:

a) sesuai dengan tujuan Dinas XYZ;

b) menetapkan sasaran keamanan informasi; atau menyediakan kerangka kerja sasaran keamanan informasi

c) memenuhi persyaratan yang berlaku terkait dengan keamanan informasi; dan

d) mencakup komitmen untuk perbaikan berkelanjutan terhadap SMKI.

Contoh Kebijakan

Kebijakan Sistem Manajamen Keamanan Informasi Instansi XYZ

Kebijakan Sistem Manajamen Keamanan_Informasi XYZ adalah :

a. Menerapkan SNI ISO 27001 sebagai sistem formal terdokumentasi untuk melindungi kerahasiaan, keutuhan dan ketersediaan informasi.
b. Instansi XYZ Menyusun objektif keamanan informasi setiap tahun dan mengukur kinerjanya setiap 6 bulan sekali.
c. Instansi XYZ berkomitment untuk memenuhi semua persyaratan yang bisa diterapkan terkait pelaksanaan keamanan informasi.
d. Instansi XYZ berkomitmen untuk peningkatan secara berkelanjutan atas SMKI

Tugas Klausul 5

1. Peserta melakukan pemetaan struktur organisasi dalam penerapan SMKI
2. Peserta menyusun Kebijakan SMKI yang akan diterapkan di organisasi masing-masing

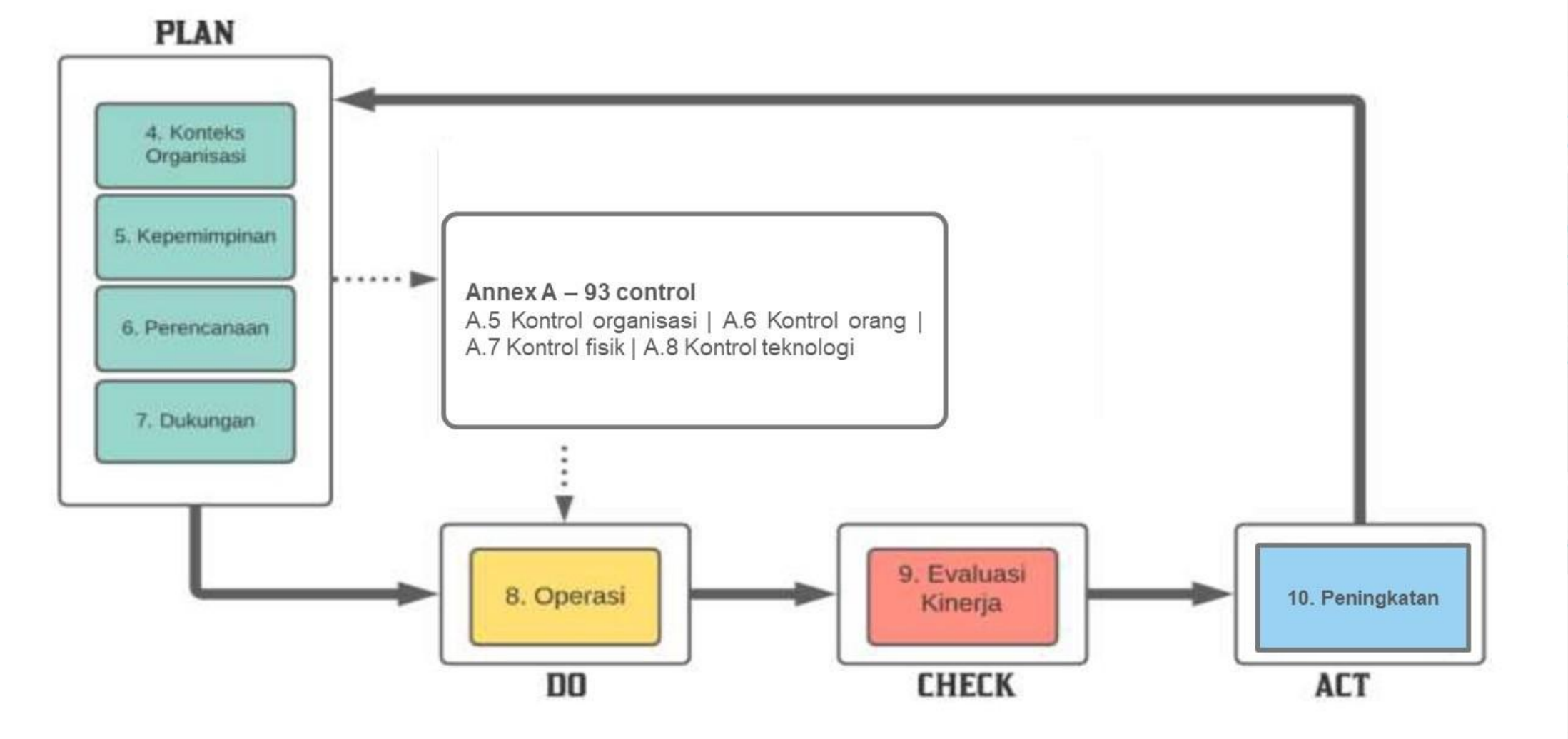
TERIMA KASIH

Sistem Manajemen Keamanan Informasi SNI ISO/IEC 27001:2022

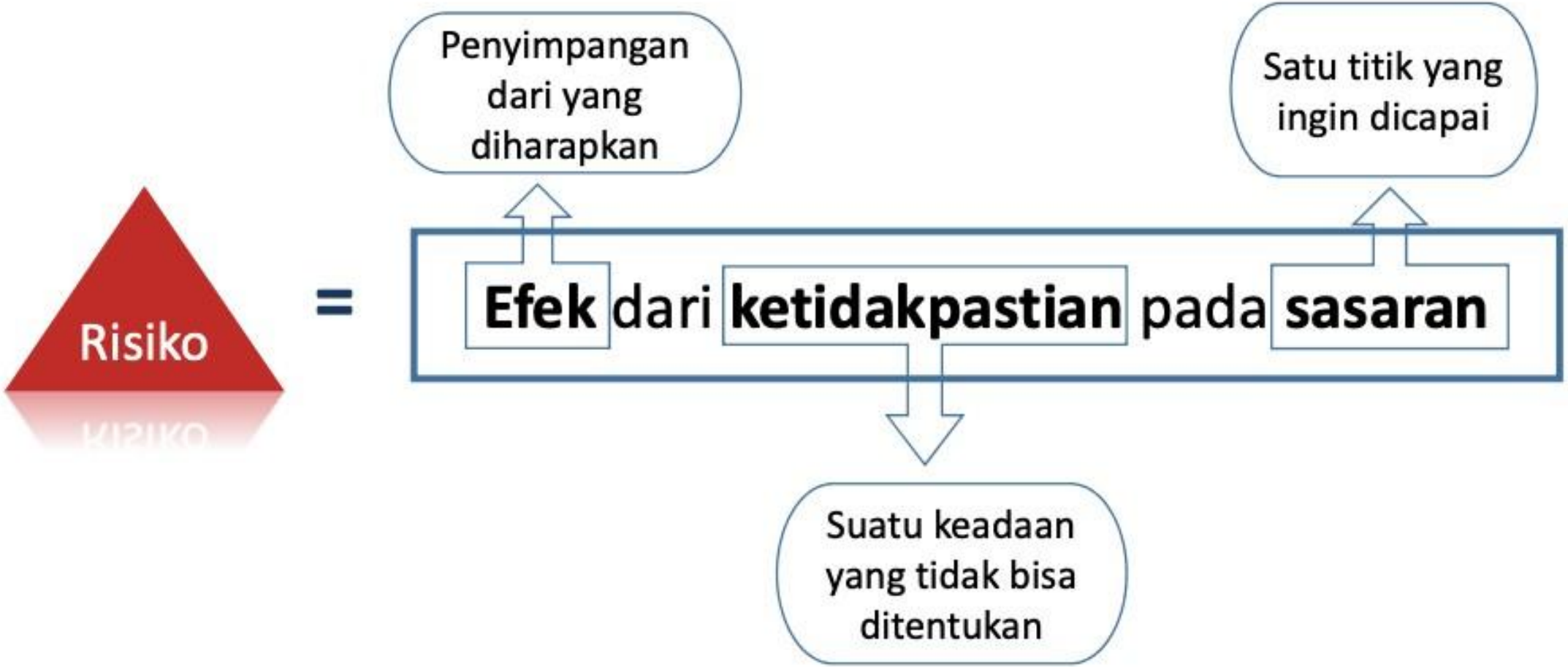
Klausul 6 Perencanaan
Klausul 7 Dukungan

Klausul 6 Perencanaan

Siklus PDCA SNI ISO/IEC 27001:2022



- Definisi Risiko



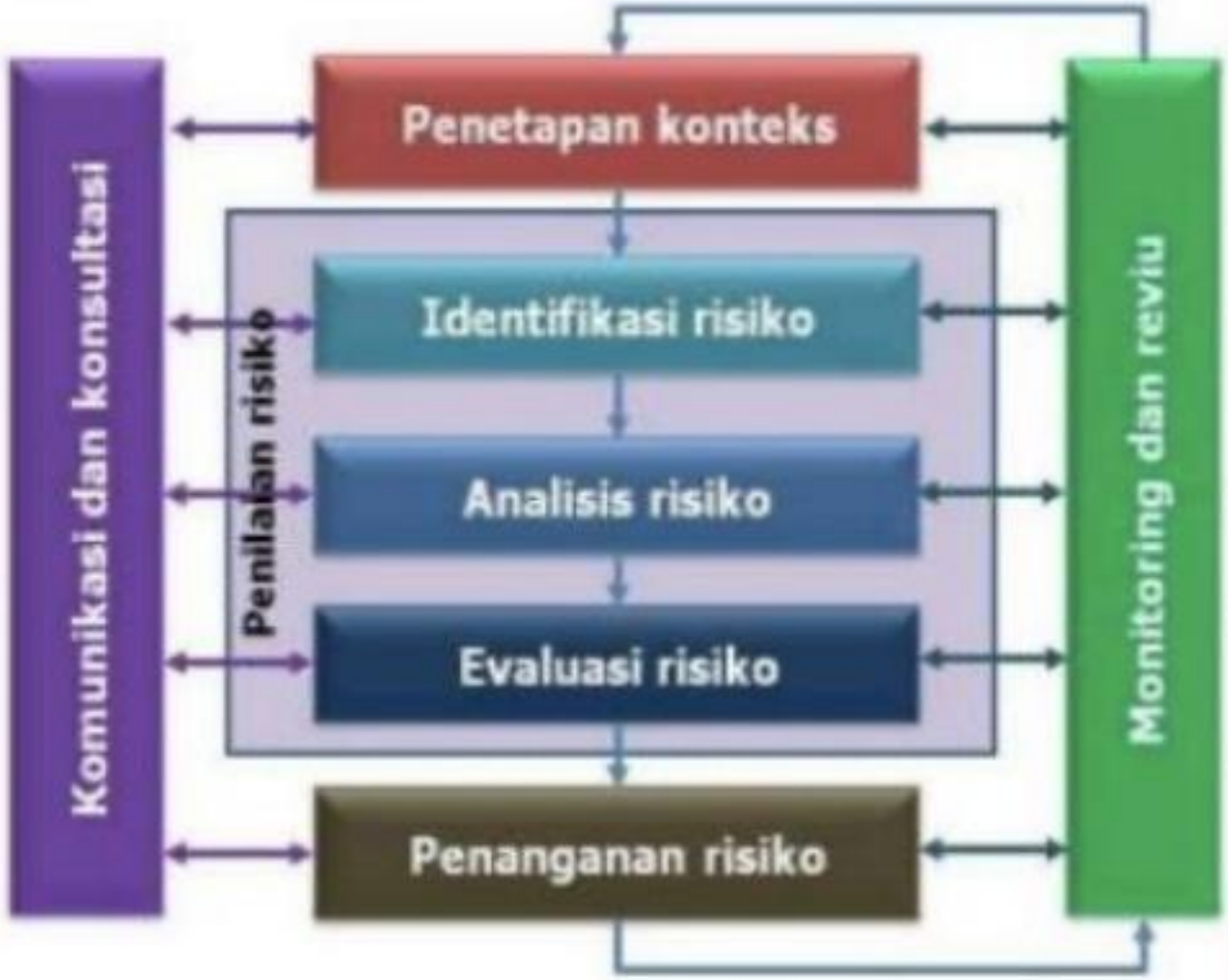
(*Effect of uncertainty on objectives* – ISO 31000)

Klausul 6.1 Tindakan untuk menangani risiko dan peluang

Ketika merencanakan SMKI, organisasi harus mempertimbangkan permasalahan dan persyaratan serta menentukan risiko dan peluang yang perlu ditangani untuk:
a) memastikan SMKI dapat mencapai manfaat yang diharapkan;
b) mencegah, atau mengurangi, efek yang tidak diinginkan;
c) mencapai perbaikan yang berkelanjutan.

Organisasi harus merencanakan:
d) tindakan untuk menangani risiko dan peluang; dan
e) bagaimana cara:

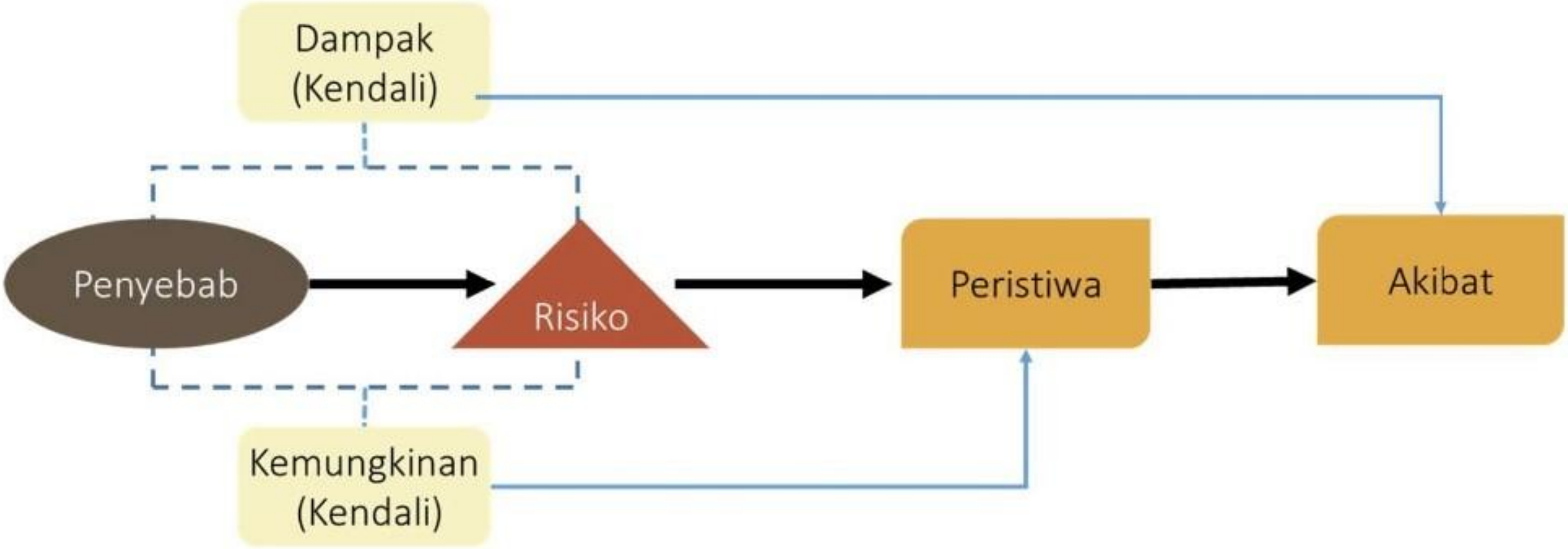
1. mengintegrasikan dan menerapkan tindakan ke dalam proses SMKI; dan
2. mengevaluasi efektivitas tindakan tersebut.



Proses Manajemen Risiko

1. **Penetapan Konteks**
   latar belakang, ruang lingkup, tujuan, dan lingkungan pengendalian
2. **Identifikasi Risiko**
   mengidentifikasi risiko, waktu, sebab, dan proses terjadinya peristiwa risiko
3. **Analisis risiko**
   mencermati risiko dan tingkat pengendalian serta menilai risiko
4. **Evaluasi risiko**
   dilakukan untuk pengambilan keputusan mengenai penanganan risiko
5. **Penanganan risiko**
   mengidentifikasi opsi penanganan risiko dan memilih opsi terbaik
6. **Monitoring dan reviu**
   memastikan penanganan dan langkah-langkah lanjutan yang diperlukan
7. **Komunikasi dan konsultasi**
   dilakukan terus menerus dengan cara mengembangkan metode komunikasi dan pelaporan kepada *stakeholder* internal maupun eksternal

Memahami Risiko



Klausul 6.1.2 Asesmen risiko keamanan informasi

Organisasi harus mendefinisikan dan mengaplikasikan proses asesmen risiko keamanan informasi yang:

Kategori / Kriteria Risiko

No	Kategori Risiko
1.	Rencana Induk SPBE Nasional
2.	Arsitektur SPBE
3.	Peta Rencana SPBE
4.	Proses Bisnis
5.	Rencana dan Anggaran
6.	Inovasi
7.	Kepatuhan terhadap Peraturan
8.	Pengadaan Barang dan Jasa
9.	Proyek Pembangunan/Pengembangan Sistem
10.	Data dan Informasi
11.	Infrastruktur
12.	Aplikasi
13.	Keamanan
14.	Layanan
15.	SDM
16.	Bencana Alam

Kriteria risiko ditentukan untuk mengevaluasi signifikansi risiko dan untuk mendukung proses pengambilan keputusan.

Kriteria risiko sebaiknya merefleksikan nilai, sasaran, dan sumber daya organisasi serta konsisten dengan kebijakan dan pernyataan tentang manajemen risiko.

Berdasarkan Permen PAN-RB No 5 Tahun 2020, kategori Risiko SPBE sudah ditentukan sebagaimana di tabel kanan.

Pernyataan Risiko

Pernyataan risiko adalah pernyataan terhadap potensi risiko yang dapat mempengaruhi tercapainya sasaran. Pernyataan potensi risiko dapat diidentifikasi dengan melalui pendekatan :

a) Data kejadian/insiden yang mengakibatkan sasaran tidak tercapai.
b) Teori ilmiah yang disampaikan para pakar
c) Pengalaman terdahulu

Contoh Pernyataan Risiko :

- Adanya celah pada pemrograman aplikasi yang mudah ditembus dari pihak luar
- Koneksi internet terganggu
- Hilangnya data pada media penyimpanan
- Perangkat server mengalami gagal fungsi

Contoh Kategori & Pernyataan Risiko

Kategori dan Pernyataan Risiko

Kategori Risiko	Pernyataan Risiko
Keamanan	Adanya celah pada pemrograman aplikasi yang mudah ditembus dari pihak luar
Infrastruktur	Koneksi internet terganggu
Data dan Informasi	Hilangnya data pada media penyimpanan
Layanan	Perangkat server mengalami gagal fungsi
...	...
...	...

Area Dampak

No	Area Dampak Risiko SPBE
1	Finansial
2	Reputasi
3	Kinerja
4	Layanan Organisasi
5	Operasional dan Aset TIK
6	Hukum dan Regulasi
7	Sumber Daya Manusia

Pernyataan Besaran Area Dampak

No	Area Dampak Risiko SPBE	Pernyataan besaran area dampak
1	Finansial	Terdapat kerugian finansial sebesar Rp. .....
2	Kinerja	Mengakibatkan target kinerja terlaksana kurang dari ..... persen
3	Layanan Organisasi	Layanan operasional terhenti sebagian
4	Operasional dan Aset TIK	Terdapat kerusakan asset sebesar Rp. .....
5	Hukum dan Regulasi	Potensi melanggar ketentuan ..... Yang dapat berakibat adanya tuntutan pidana/perdata
6	Sumber Daya Manusia	Berkurangnya tenaga kerja yang kompeten

Level Kemungkinan (*Likelihood*)

Level kemungkinan terjadinya Risiko (likelihood/ frequency), yaitu besarnya peluang atau frekuensi suatu Risiko akan terjadi. Pengukurannya bisa menggunakan pendekatan statistik (probability), frekuensi kejadian persatuan waktu (hari, minggu, bulan, tahun) , atau dengan expert judgement

Level Kemungkinan		Persentase Kemungkinan Terjadinya dalam Satu Tahun	Jumlah Frekuensi Kemungkinan Terjadinya dalam Satu Tahun
1	Hampir Tidak Terjadi	X≤5%	X < 2 kali
2	Jarang Terjadi	5%<X≤10%	2 ≤ X ≤ 5 kali
3	Kadang-Kadang Terjadi	10%<X≤20%	6 ≤ X ≤ 9 kali
4	Sering Terjadi	20%<X≤50%	10 ≤ X ≤ 12 kali
5	Hampir Pasti Terjadi	X>50%	> 12 kali

Level Dampak Terjadinya Risiko

Dampak dan probabilitas risiko-risiko ini ditentukan karena berkaitan dengan Keamanan Informasi (CIA). Berdasarkan kriteria penerimaan risiko organisasi, yang merupakan fungsi dari selera terhadap risiko organisasi, organisasi menentukan pendekatan untuk menangani risiko ini.

Nilai	Tingkat Dampak
1	Tidak Signifikan
2	Kurang Signifikan
3	Cukup Signifikan
4	Signifikasn
5	Sangat Signifikan

Kriteria Dampak Risiko

Area Dampak	Level Dampak				
	1	2	3	4	5
	Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Finansial	Tidak terdapat kerugian finansial	terdapat kerugian/biaya yang harus dikeluarkan hingga Rp. 50.000.000,-	terdapat kerugian/biaya yang harus dikeluarkan Rp. 50.000.000,- hingga Rp. 250.000.000,-	terdapat kerugian/biaya yang harus dikeluarkan Rp. 250.000.000,- Rp. 500.000.000,-	terdapat kerugian/biaya yang harus dikeluarkan lebih dari Rp. 500.000.000,-
Reputasi	Terdapat pemberitaan negatif namun tidak mengakibat penurunan kepercayaan	Terdapat pemberitaan negatif yang dapat mempengaruhi tingkat kepercayaan *stakeholder*	terdapat pemberitaan negatif yang terus menurunkan kepercayaan *stakeholder*	hilangnya kepercayaan *stakeholder*	Stakeholder sama sekali tidak percaya
Kinerja	Tidak Menimbulkan penurunan kinerja	Penurunan kinerja sampai 30%	Penurunan kinerja sampai 50%	Penurunan kinerja sampai 70%	Penurunan kinerja sampai 90%
Operasional dan Aset TIK	Terdapat gangguan namun tidak mengakibatkan proses bisnis teraganggu	terdapat gangguan yang menyebabkan 1 mata rantai proses bisnis terganggu	terdapat gangguan yang menyebabkan lebih dari 1 mata rantai proses bisnis terganggu	terdapat gangguan yang menyebabkan seluruh proses bisnis terganggu	terjadi kelumpuhan pada proses bisnis
Hukum dan Regulasi	Tidak Menimbulkan dampak hukum	Menimbulkan dampak hukum kategori ringan	menimbulkan dampak hukum kategori sedang	menimbulkan dampak hukum kategori berat	Menimbulkan kasus Hukum Tindak pidana
Sumber Daya Manusia	Seluruh SDM telah sesuai dengan kebutuhan dan pengembangan kapasitas SDM	Sebagaian Besar / 90% SDM telah sesuai dengan kebutuhan dan pengembangan kapasitas SDM	sebagian kecil / 60% SDM telah sesuai dengan kebutuhan dan pengembangan kapasitas SDM	SDM belum sesuai / 30% dengan kebutuhan dan pengembangan kapasitas SDM	SDM tidak sesuai dengan kebutuhan dan pengembangan kapasitas SDM
Layanan Organisasi	Menimbulkan penundaan layanan organisasi maksimal 24 jam	Menimbulkan penundaan layanan organisasi maksimal 2 x 24 jam	Menimbulkan penundaan layanan organisasi maksimal 3 x 24 jam	Menimbulkan penundaan layanan organisasi maksimal 5 x 24 jam	Menimbulkan penundaan layanan organisasi lebih dari 5 x 24 jam

MATRIKS ANALISIS RISIKO & LEVEL RISIKO

Nilai Risiko

Nilai Risiko merupakan kombinasi antara tingkat kemungkinan terjadinya risiko dan tingkat dampak yang direpresentasikan dengan angka , yang dirumuskan sebagai berikut :

Nilai Risiko = Level Kemungkinan x Level Dampak

Nilai resiko selanjutnya dikelompokkan dalam rentang nilai tertentu untuk memudahkan saat dilakukan seleksi prioritas penanganan risiko

Matriks Analisis Risiko

Matriks Analisis Risiko			Level Dampak				
			1	2	3	4	5
5x5			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Level Kemungkinan	5	Hampir Pasti Terjadi	9	15	18	23	25
	4	Sering Terjadi	6	12	16	19	24
	3	Kadang-Kadang Terjadi	4	10	14	17	22
	2	Jarang Terjadi	2	7	11	13	21
	1	Hampir Tidak Terjadi	1	3	5	8	20

Level Risiko

Level Risiko SPBE

Level Risiko	Rentang Besaran Risiko	Simbol Warna
Sangat Rendah	1 - 5	Biru
Rendah	6 - 10	Hijau
Sedang	11 – 15	Kuning
Tinggi	16 – 20	Jingga
Sangat Tinggi	21 - 25	Merah

Rentang Nilai Risiko	Pernyataan Rentang Nilai Risiko	Simbol Warna	Tindakan yang diambil
1 - 5	Sangat Rendah	Biru	Tidak diperlukan tindakan
6 - 10	Rendah	Hijau	Diambil tindakan jika diperlukan
11 – 15	Sedang	Kuning	Diambil tindakan jika sumber daya tersedia
16 – 20	Tinggi	Jingga	Diperlukan tindakan untuk mengelola risiko
21 - 25	Sangat Tinggi	Merah	Diperlukan tindakan segera untuk mengelola risiko

Matriks Analisis Risiko Versi 31000 (Intermezzo)

Matriks Analisis Risiko			Level Dampak				
			1	2	3	4	5
			Tidak Signifikan	Kecil	Sedang	Besar	Katastrope
Level Kemungkinan	5	Hampir Pasti terjadi	5	10	15	20	25
	4	Sering Terjadi	4	8	12	16	20
	3	Kadang Terjadi	3	6	9	12	15
	2	Jarang Terjadi	2	4	6	8	10
	1	Hampir Tidak terjadi	1	2	3	4	5

Rendah (Hijau), Menengah (Kuning), Tinggi (Orange), Sangat Tinggi (Merah)

Selera Risiko

Selera Risiko bertujuan untuk memberikan acuan dalam penentuan ambang batas minimum terhadap Besaran Risiko yang harus ditangani untuk setiap Kategori Risiko baik Risiko Positif maupun Risiko Negatif. Penentuan Selera Risiko ini dapat disesuaikan dengan kompleksitas Risiko serta konteks internal dan eksternal masing-masing Instansi.

No	Kategori Risiko	Besaran Risiko Minimum Yang ditangani	
		Risiko Positif	Risiko Negatif
1	Peta Rencana	x	16
2	Proyek Pembangunan/Pengembangan Sistem	x	20
3	Data dan Informasi	x	10
4	Infrastruktur	x	16
5	Keamanan	x	16
6	Keamanan	x	16
7	SDM	x	...

Risk Register

Pengisian kolom awal pada saat memulai identifikasi risiko, terdiri dari :

1. **Jenis Risiko**, Jenis Risiko terbagi menjadi Risiko positif dan Risiko negatif. Dalam melakukan identifikasi Risiko, Risiko dituliskan ke dalam masing-masing jenis Risiko SPBE.
2. **Kejadian (Pernyataan Risiko),** Kejadian dapat diidentifikasi dari terjadinya suatu peristiwa yang menimbulkan Risiko SPBE yang diperoleh dari riwayat peristiwa dan/atau prediksi terjadinya peristiwa di masa yang akan datang.
3. **Jenis Ancaman**, Jenis Ancaman mengacu kepada probabilitas ancaman keamanan informasi yang terganggu dari bagian Confidentiality, Integrity, atau Availability yang diidentifikasi dari pernyataan risiko
4. **Penyebab**, Penyebab dapat diidentifikasi dari akar masalah yang menjadi pemicu munculnya Risiko. Penyebab dapat berasal dari lingkungan internal maupun eksternal Instansi Pusat dan Pemerintah Daerah. Identifikasi penyebab akan membantu menemukan tindakan yang tepat untuk menangani Risiko.
5. **Kategori,** Penentuan Kategori Risiko didasarkan pada penyebab dari munculnya Risiko.
6. **Dampak,** Dampak dapat diidentifikasi dari pengaruh atau akibat yang timbul dari Risiko SPBE.
7. **Area Dampak**, Penentuan Area Dampak Risiko didasarkan pada dampak yang telah teridentifikasi.

Risk Register

Identifikasi Risiko						
Jenis Risiko	**Kejadian (Pernyataan)**	**Jenis Ancaman (C/I/A)**	**Penyebab**	**Kategori**	**Dampak**	**Dampak Area**
Positif						
Negatif	Aplikasi ter-deface	Availability	Adanya celah pada pemrograman aplikasi yang mudah ditembus pihak luar	Keamanan	Operasional organisasi terganggu	Kinerja

Risk Register

Pengisian kolom selanjutnya yaitu kolom analisis risiko, terdiri dari :

a. Sistem Pengendalian
   - Sistem pengendalian internal mencakup perangkat manajemen yang dapat menurunkan/meningkatkan level Risiko dalam rangka pencapaian sasaran
   - Sistem pengendalian internal dapat berupa *Standard Operating Procedure* (SOP), pengawasan melekat, reviu berjenjang, regulasi, dan pemantauan rutin yang dilaksanakan terkait Risiko tersebut.

b. Level Kemungkinan

c. Level Dampak

d. Besaran Risiko (Nilai Risiko) dan Level Risiko

Risk Register

Analisis Risiko				
Sistem Pengendalian	Kemungkinan	Dampak	Nilai Risiko	Level Risiko
	Level	Level		
Penyusunan prosedur Penetration Test	5	4	23	Sangat Tinggi

Risk Register

Pengisian kolom selanjutnya yaitu kolom rencana penanganan risiko. Terdiri dari Opsi Penanganan Risiko, Rencana Aksi Penanganan Risiko, Keluaran, Jadwal Implementasi, dan Penanggung Jawab. Adapun Opsi Penanganan Risiko (Negatif) terdiri dari :

- **Eskalasi Risiko**: Eskalasi risiko dipilih jika **Risiko berada di luar atau melampaui wewenang**. Opsi ini dilakukan dengan **memindahkan tanggung jawab** penanganan Risiko ke unit kerja yang lebih tinggi.
- **Mitigasi Risiko**: Mitigasi risiko dilakukan dengan cara **mengurangi level** kemungkinan dan/atau level dampak dari Risiko
- **Transfer Risiko**: Transfer risiko dipilih jika terdapat kekurangan sumber daya untuk mengelola Risiko. Opsi ini dilakukan dengan cara mengalihkan kepemilikan risiko kepada pihak lain untuk melakukan pengelolaan dan pertanggungjawaban terhadap Risiko.
- **Penghindaran Risiko**: Penghindaran risiko dilakukan dengan mengubah perencanaan, penganggaran, program, dan kegiatan, atau aspek lainnya untuk mencapai sasaran SPBE.
- **Penerimaan Risiko**: Opsi ini dipilih jika biaya dan usaha penanganan lebih tinggi diandingkan manfaat yang di dapat, Tindakan yang di ambil adalah membiarkan risiko tersebut terjadi apadanya

Risk Register

Rencana Penanganan Risiko				
Opsi Penanganan	**Rencana Aksi Penanganan Risiko**	**Keluaran**	**Jadwal Implementasi**	**Penanggung Jawab**
Mitigasi	Melakukan Penetration Test dan mencatat hasil Penetration Test	Laporan hasil Penetration Test	Pada saat perbaikan	Bidang Infrastruktur, Keamanan dan Informasi

Risk Register

ID	Identifikasi Risiko							Analisis Risiko					Rencana Penanganan Risiko				
	Jenis Risiko	Kejadian (Pernyataan)	Jenis Ancaman (C/I/A)	Penyebab	Kategori	Dampak	Dampak Area	Sistem Pengendalian	Kemungkinan	Dampak	Nilai Risiko	Level Risiko	Opsi Penanganan Risiko	Rencana Aksi Penanganan Risiko	Keluaran	Jadwal Implementasi	Penanggung Jawab
									Level	Level							
1	Positif																
1	Negatif	Aplikasi ter-deface	Availability	Adanya celah pada pemrograman aplikasi yang mudah ditembus pihak luar	Keamanan	Operasional organisasi terganggu	Kinerja	Penyusunan prosedur Penetration Test	5	4	23	Sangat Tinggi	Mitigasi	Melakukan Penetration Test dan mencatat hasil Penetration Test	Laporan hasil Penetration Test	Pada saat perbaikan	Bidang Infrastruktur, Keamanan dan Informasi

***Hanya Contoh**

Klausul 6.1.3 Penanganan risiko keamanan informasi

Organisasi harus menetapkan dan menerapkan proses penanganan risiko keamanan informasi untuk:

Informasi terdokumentasi dipelihara

Statement of Applicability (SOA)

Dokumentasi Analisis Kontrol Implementasi SMKI

Pernyataan Kontrol terhadap Annex A SNI ISO/IEC 27001:2022

4 Domain dan 93 Kontrol Keamanan Informasi

Statement of Applicability (SOA)

Pernyataan Pemberlakuan

Versi 1.0
Tanggal 03/10/2022
Ruang Lingkup SMKI

ISO/IEC 27001:2013 Statement of Applicability				Apakah kontrol bisa diaplikasikan? (YA / TIDAK)	Alasan / Keterangan pemilihan kendali annex	Referensi dokumen/bukti dukung (Kebijakan, prosedur, formulir)	Keterangan Tambahan (jika Ada)
Area	**Section**	**Control**	**Deskripsi Kontrol**				
A.5 Kebijakan keamanan informasi							
	A.5.1 Arahan manajemen untuk keamanan informasi	A.5.1.1 Kebijakan untuk keamanan informasi	Kendali Seperangkat kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak luar yang terkait.				
		A.5.1.2 Reviu kebijakan keamanan informasi	Kendali Kebijakan untuk keamanan informasi harus direviu pada interval waktu terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan dan keefektifan yang berkelanjutan				
A.6 Organisasi keamanan informasi							
	A.6.1 Organisasi internal	A.6.1.1 Peran dan tanggung jawab keamanan informasi	Kendali Semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan.				
		A.6.1.2 Pemisahan tugas	Kendali Tugas dan area tanggung jawab yang bertentangan harus dipisahkan (dijabat oleh personel yang berbeda) untuk mengurangi kemungkinan dari modifikasi yang tidak sah atau tidak sengaja atau penyalahgunaan aset organisasi.				
		A.6.1.3 Hubungan dengan pihak berwenang	Kendali Hubungan baik dengan pihak berwenang terkait harus dipelihara.				

Klausul 6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

Organisasi harus menetapkan sasaran keamanan informasi pada fungsi dan level yang relevan. Sasaran keamanan informasi harus:

a) konsisten dengan kebijakan keamanan informasi;
b) dapat diukur (jika dapat dipraktikkan);
c) mempertimbangkan persyaratan keamanan informasi yang dapat diaplikasikan, dan hasil dari asesmen risiko dan penanganan risiko;
d) termonitorkan;
e) terkomunikasikan;
f) termutakhirkan dengan tepat;
g) tersedia sebagai informasi terdokumentasi.

Organisasi harus menyimpan informasi terdokumentasi mengenai sasaran keamanan informasi.

Klausul 6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

Ketika merencanakan bagaimana mencapai sasaran keamanan informasinya, organisasi harus menentukan:

Contoh sasaran SMKI: Dilakukan pencadangan data (*backup*) secara rutin minimum 1 kali seminggu.

Informasi terdokumentasi dipelihara

Contoh Sasaran SMKI

Sasaran SMKI
- Daftar inventaris sistem aplikasi diperbaharui setiap tahunnya - Dilakukan pencadangan basis data (*Back up data base)* secara rutin sesuai periode yang ditetapkan - Dilakukan pembaharuan anti virus secara rutin sesuai periode yang ditetapkan - Tingkat kegagalan sistem aplikasi maksimal 5% setiap tahunnya
- Daftar inventaris aset server dan jaringan diperbaharui setiap tahunnya - Serangan dari luar teridentifikasi setiap tahunnya - Tingkat kegagalan server maksimal 5% setiap tahunnya
- Dilakukan perawatan dan monitoring kondisi komputer pribadi dan alat pendukungnya secara berkala - Daftar inventaris aset komputer pribadi dan alat pendukungnya diperbaharui setiap tahunnya

6.3 Perencanaan perubahan

Ketika organisasi menentukan kebutuhan perubahan atas sistem manajemen keamanan informasi, perubahan tersebut harus dilakukan dengan cara yang terencana.

Klausul 7 Dukungan

Klausul 7.1 Sumber Daya

"Organisasi harus menentukan dan menyediakan **sumber daya** yang dibutuhkan untuk penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI".

- Sumber Daya Manusia
- Sumber Daya Teknis
- Sumber Daya Keuangan

Sumber daya manusia, misalnya manajemen puncak, personel yang terlibat dalam penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI;

Sumber daya teknis, misalnya sistem dan infrastruktur yang mendukung implementasi SMKI;

Sumber daya keuangan, termasuk dana untuk proyek dan dana untuk pengoperasian penerapan SMKI.

Klausul 7.2 Kompetensi

Organisasi **Harus** :

a. menentukan kompetensi yang diperlukan untuk personel yang melakukan pekerjaan di bawah kendali organisasi yang mempengaruhi kinerja keamanan informasi organisasi;

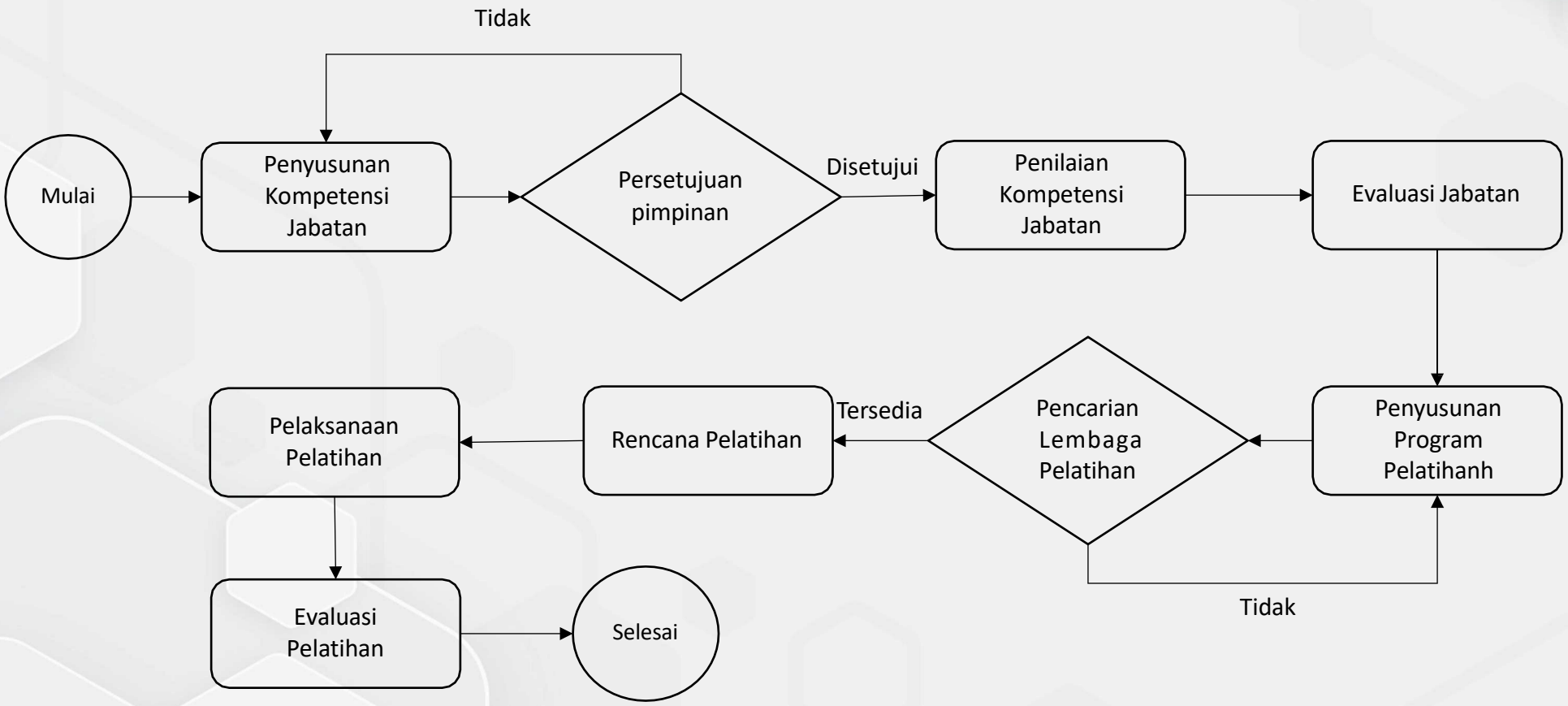
b. memastikan bahwa personel ini kompeten berdasarkan pendidikan, pelatihan, atau pengalaman yang sesuai;

c. apabila memungkinkan, mengambil tindakan untuk memperoleh kompetensi yang diperlukan, dan mengevaluasi efektivitas tindakan yang diambil; dan

d. menyimpan informasi terdokumentasi yang sesuai sebagai alat bukti kompetensi

CATATAN : Tindakan yang bisa diterapkan dapat meliputi, misal: penyediaan pelatihan, bimbingan, atau penugasan kembali temadap karyawan yang ada; atau merekrut atau mengontrak personel yang kompeten

Flow Pengelolaan Kompetensi



Klausul 7.2 Kompetensi

Peran/ Jabatan	Deskripsi Pekerjaan	Persyaratan Komptensi		
		Pendidikan	Pengalaman Kerja	Pelatihan
Web Programmer	Membuat aplikasi menggunakan framework PHP ..	S1 Teknologi Informasi, …	Membuat aplikasi XYZ di PT. ABC	Framework PHP version ..

Klausul 7.3 Kepedulian

Personel yang bekerja di bawah kendali organisasi harus peduli terhadap:

a) kebijakan keamanan informasi;

b)kontribusinya terhadap efektivitas SMKI, termasuk manfaat peningkatan kinerja keamanan informasi; dan

c) implikasi dari ketidaksesuaian dengan persyaratan SMKI.

Annex A.7.2.2

Sosialisasi

Poster/Media cetak

Socmed

Organisasi **harus** menentukan kebutuhan berkomunikasi internal dan eksternal yang relevan dengan SMKI yang mencakup:

- apa yang akan dikomunikasikan ?
- kapan berkomunikasi ?
- dengan siapa berkomunikasi ?
- proses yang dipengaruhi oleh komunikasi tersebut
- siapa yang harus mengomunikasikan

Klausul 7.4 Komunikasi

No	Materi Komunikasi	Periode Komunikasi	Target Penerima	Media Komunikasi	**PIC**
1	Sasaran SMKI	Tiap Tahun	Semua Pegawai	Teleconference	Koordinator SMKI

Klausul 7.5 Informasi Terdokumentasi

7.5.1 Umum

Organisasi SMKI harus mencakup:

a) informasi terdokumentasi yang disyaratkan oleh Standar ini; dan

b)informasi terdokumentasi yang ditentukan oleh organisasi, sesuai yang diperlukan untuk efektivitas SMKI.

CATATAN cakupan informasi terdokumentasi untuk SMKI dapat berbeda antara satu organisasi dengan organisasi yang lain karena:

1) ukuran organisasi dan jenis kegiatan, proses, produk dan layanannya;
2) kompleksitas proses dan interaksinya; dan
3) kompetensi personelnya.

ISO 10013:2021

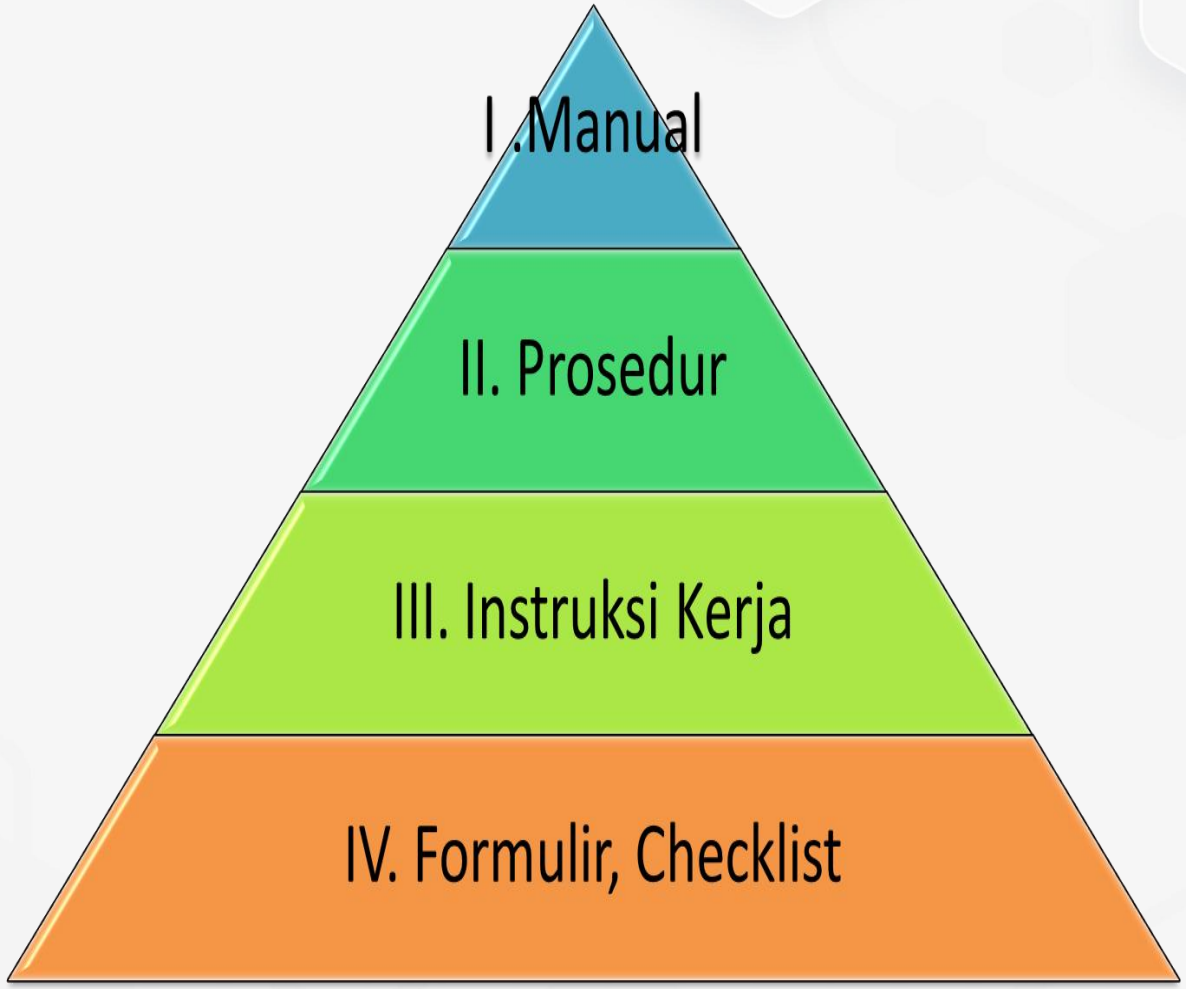
Klausul 7.5 Informasi Terdokumentasi

komitmen dan kebijakan , peraturan perundangan Dll

Rangakain Kegiatan SMKI, Uraian Kebijakan dll

Bagaimana/Cara/Langkah2 seseorang melaksanakan tugas

Bukti, Atau rekaman dokumen



Klausul 7.5 Informasi Terdokumentasi

7.5.2 Membuat dan memperbarui

Ketika membuat dan memperbarui informasi terdokumentasi organisasi **harus** memastikan kecukupan hal-hal berikut ini:

a) identifikasi dan deskripsi (misal judul, tanggal, penulis, atau nomor referensi);

b) format (misal bahasa, versi perangkat lunak, grafis) dan media (misal kertas, elektronik); dan

c) reviu dan persetujuan untuk kesesuaian dan kecukupan.

Klausul 7.5 Informasi Terdokumentasi

7.5.3 Pengendalian informasi terdokumentasi

Informasi terdokumentasi yang dibutuhkan oleh SMKI dan Standar ini harus dikendalikan untuk memastikan:

- informasi terdokumentasi tersedia dan cocok untuk digunakan, di mana dan kapan saja diperlukan; dan
- informasi terdokumentasi cukup terlindungi (misal dari terungkapnya kerahasiaan, penyalahgunaan, atau hilangnya integritas).

Klausul 7.5 Informasi Terdokumentasi

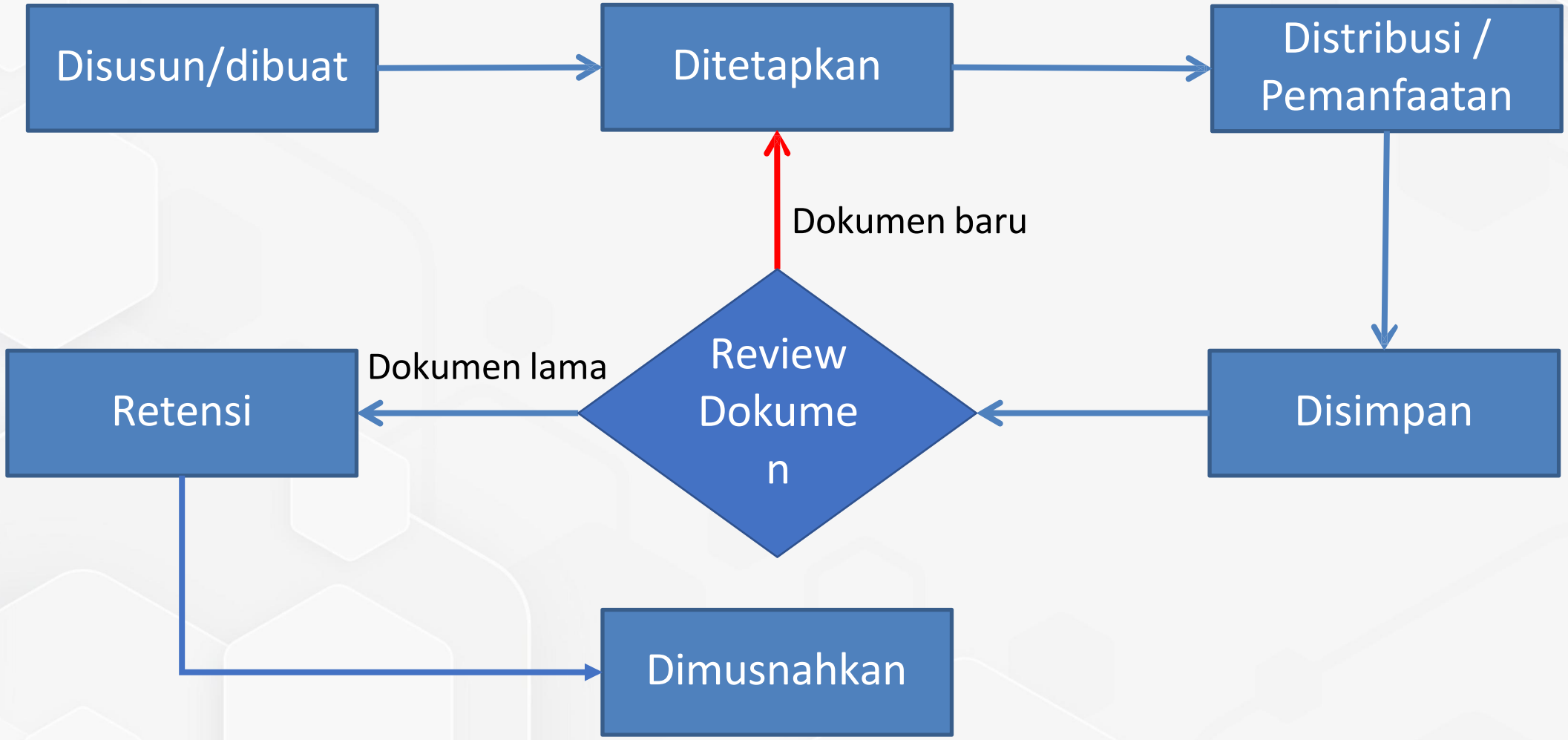
Untuk pengendalian informasi terdokumentasi, organisasi harus menangani kegiatan- kegiatan berikut, jika dapat diterapkan:

- distribusi, akses, pengambilan dan penggunaan;
- penyimpanan dan pemeliharaan, termasuk pemeliharaan keterbacaan *(legibility)*;
- pengendalian perubahan, misal pengendalian versi *(version control)*; dan
- retensi (*retention*) dan disposisi *(disposition)*.

Informasi terdokumentasi yang bersumber dari luar, yang menurut organisasi diperlukan untuk perencanaan dan operasi SMKI, harus diidentifikasi kesesuaiannya dan dikendalikan.

CATATAN Akses mencakup keputusan terkait izin dan kewenangan untuk melihat informasi terdokumentasi saja, atau melihat dan mengubah informasi terdokumentasi, dll.

Siklus dokumen



Tugas Klausul 6

1. Buatlah identifikasi Level Kemungkinan & Kriteria Dampak Risiko
2. Buatlah Dokumen Risk Register

Tugas Klausul 7

1. mengidentifikasi kebutuhan kompetensi untuk keamanan informasi di masing- masing instansi (7.2)
2. Mengidentifikasi bentuk komunikasi dan kepedulian keamanan informasi di masing-masing instansi (7.4)

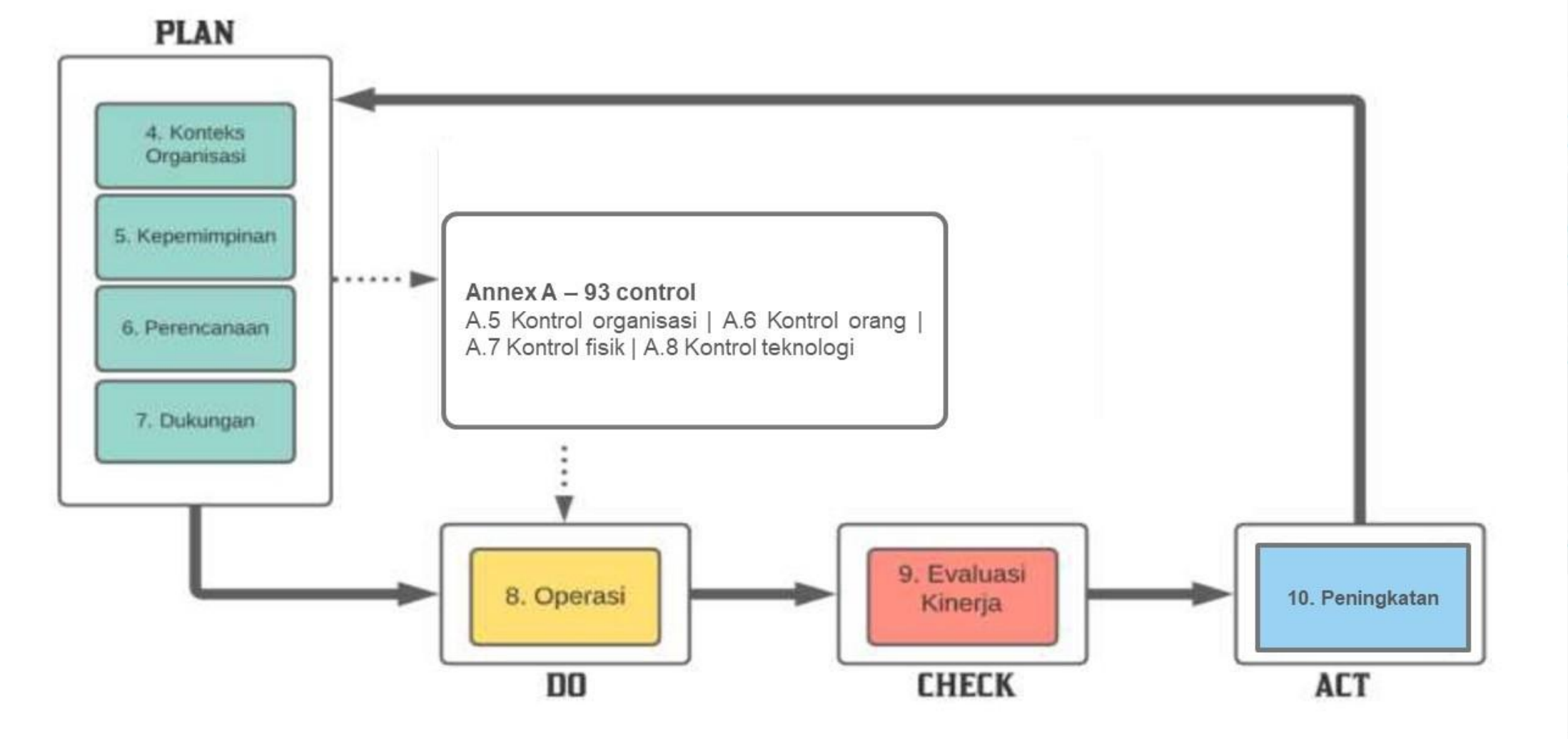
TERIMA KASIH

Sistem Manajemen Keamanan Informasi SNI ISO/IEC 27001:2022

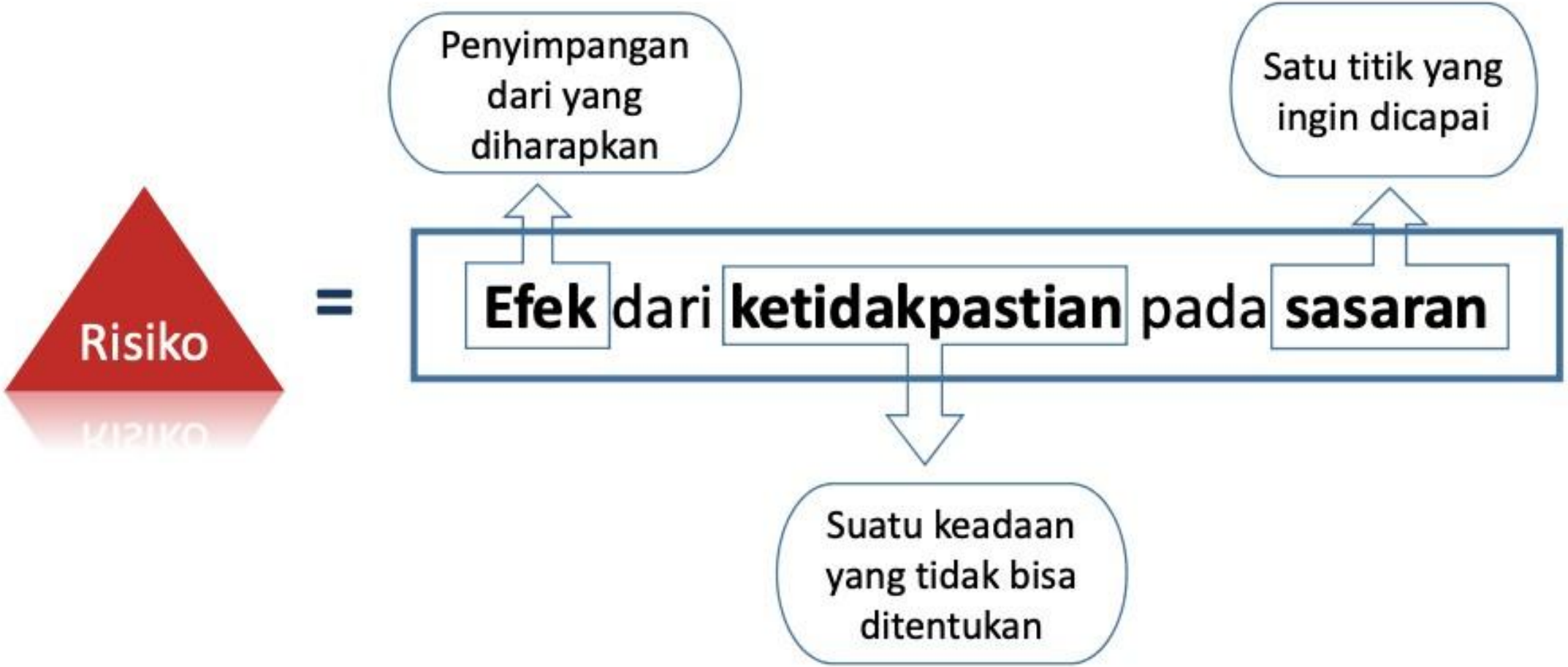
Klausul 6 Perencanaan
Klausul 7 Dukungan

Klausul 6 Perencanaan

Siklus PDCA SNI ISO/IEC 27001:2022



- Definisi Risiko



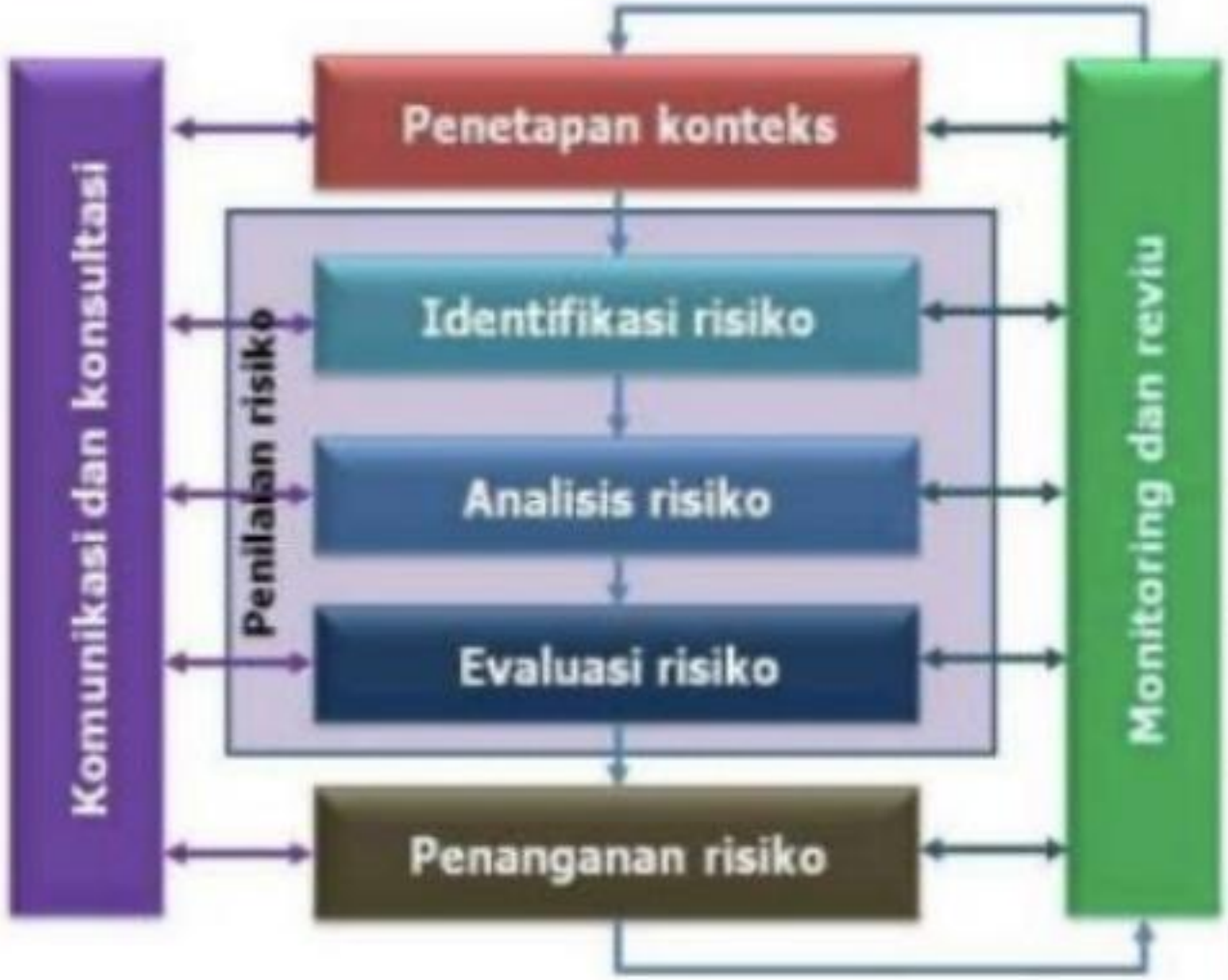
(*Effect of uncertainty on objectives* – ISO 31000)

Klausul 6.1 Tindakan untuk menangani risiko dan peluang

Ketika merencanakan SMKI, organisasi harus mempertimbangkan permasalahan dan persyaratan serta menentukan risiko dan peluang yang perlu ditangani untuk:
a) memastikan SMKI dapat mencapai manfaat yang diharapkan;
b) mencegah, atau mengurangi, efek yang tidak diinginkan;
c) mencapai perbaikan yang berkelanjutan.

Organisasi harus merencanakan:
d) tindakan untuk menangani risiko dan peluang; dan
e) bagaimana cara:

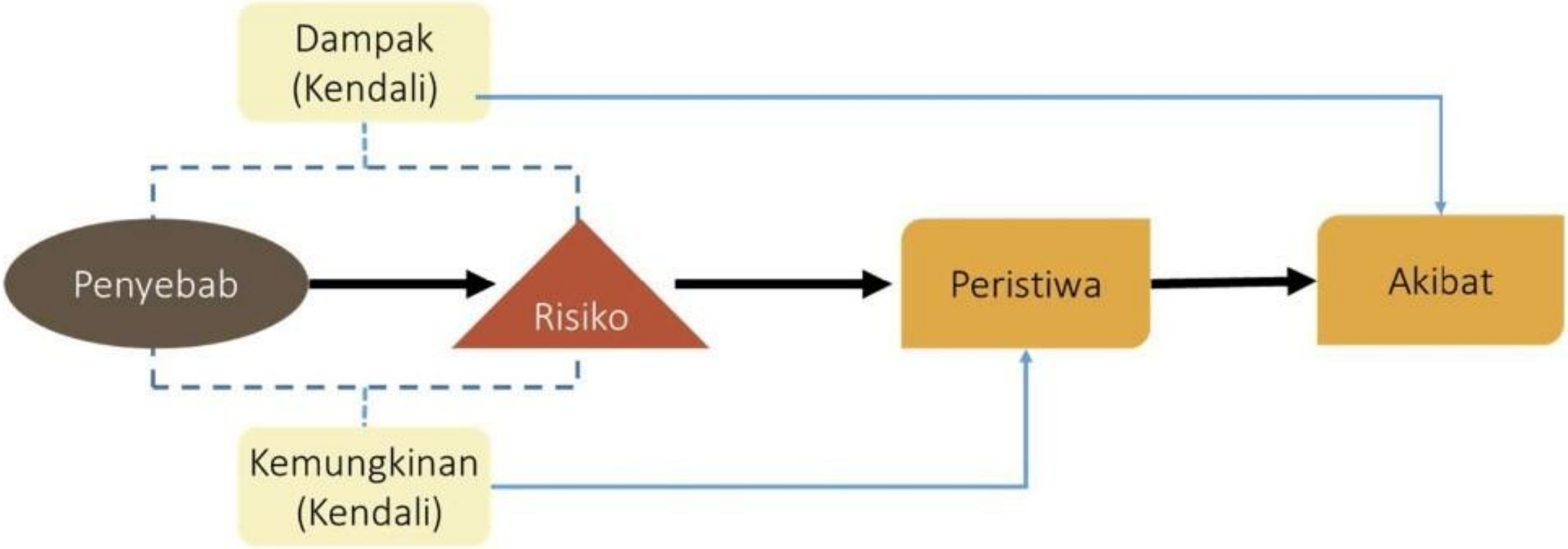
1. mengintegrasikan dan menerapkan tindakan ke dalam proses SMKI; dan
2. mengevaluasi efektivitas tindakan tersebut.



Proses Manajemen Risiko

1. **Penetapan Konteks**
   latar belakang, ruang lingkup, tujuan, dan lingkungan pengendalian
2. **Identifikasi Risiko**
   mengidentifikasi risiko, waktu, sebab, dan proses terjadinya peristiwa risiko
3. **Analisis risiko**
   mencermati risiko dan tingkat pengendalian serta menilai risiko
4. **Evaluasi risiko**
   dilakukan untuk pengambilan keputusan mengenai penanganan risiko
5. **Penanganan risiko**
   mengidentifikasi opsi penanganan risiko dan memilih opsi terbaik
6. **Monitoring dan reviu**
   memastikan penanganan dan langkah-langkah lanjutan yang diperlukan
7. **Komunikasi dan konsultasi**
   dilakukan terus menerus dengan cara mengembangkan metode komunikasi dan pelaporan kepada *stakeholder* internal maupun eksternal

Memahami Risiko



Klausul 6.1.2 Asesmen risiko keamanan informasi

Organisasi harus mendefinisikan dan mengaplikasikan proses asesmen risiko keamanan informasi yang:

Kategori / Kriteria Risiko

No	Kategori Risiko
1.	Rencana Induk SPBE Nasional
2.	Arsitektur SPBE
3.	Peta Rencana SPBE
4.	Proses Bisnis
5.	Rencana dan Anggaran
6.	Inovasi
7.	Kepatuhan terhadap Peraturan
8.	Pengadaan Barang dan Jasa
9.	Proyek Pembangunan/Pengembangan Sistem
10.	Data dan Informasi
11.	Infrastruktur
12.	Aplikasi
13.	Keamanan
14.	Layanan
15.	SDM
16.	Bencana Alam

Kriteria risiko ditentukan untuk mengevaluasi signifikansi risiko dan untuk mendukung proses pengambilan keputusan.

Kriteria risiko sebaiknya merefleksikan nilai, sasaran, dan sumber daya organisasi serta konsisten dengan kebijakan dan pernyataan tentang manajemen risiko.

Berdasarkan Permen PAN-RB No 5 Tahun 2020, kategori Risiko SPBE sudah ditentukan sebagaimana di tabel kanan.

Pernyataan Risiko

Pernyataan risiko adalah pernyataan terhadap potensi risiko yang dapat mempengaruhi tercapainya sasaran. Pernyataan potensi risiko dapat diidentifikasi dengan melalui pendekatan :

a) Data kejadian/insiden yang mengakibatkan sasaran tidak tercapai.
b) Teori ilmiah yang disampaikan para pakar
c) Pengalaman terdahulu

Contoh Pernyataan Risiko :

- Adanya celah pada pemrograman aplikasi yang mudah ditembus dari pihak luar
- Koneksi internet terganggu
- Hilangnya data pada media penyimpanan
- Perangkat server mengalami gagal fungsi

Contoh Kategori & Pernyataan Risiko

Kategori dan Pernyataan Risiko

Kategori Risiko	Pernyataan Risiko
Keamanan	Adanya celah pada pemrograman aplikasi yang mudah ditembus dari pihak luar
Infrastruktur	Koneksi internet terganggu
Data dan Informasi	Hilangnya data pada media penyimpanan
Layanan	Perangkat server mengalami gagal fungsi
...	...
...	...

Area Dampak

No	Area Dampak Risiko SPBE
1	Finansial
2	Reputasi
3	Kinerja
4	Layanan Organisasi
5	Operasional dan Aset TIK
6	Hukum dan Regulasi
7	Sumber Daya Manusia

Pernyataan Besaran Area Dampak

No	Area Dampak Risiko SPBE	Pernyataan besaran area dampak
1	Finansial	Terdapat kerugian finansial sebesar Rp. .....
2	Kinerja	Mengakibatkan target kinerja terlaksana kurang dari ..... persen
3	Layanan Organisasi	Layanan operasional terhenti sebagian
4	Operasional dan Aset TIK	Terdapat kerusakan asset sebesar Rp. .....
5	Hukum dan Regulasi	Potensi melanggar ketentuan ..... Yang dapat berakibat adanya tuntutan pidana/perdata
6	Sumber Daya Manusia	Berkurangnya tenaga kerja yang kompeten

Level Kemungkinan (*Likelihood*)

Level kemungkinan terjadinya Risiko (likelihood/ frequency), yaitu besarnya peluang atau frekuensi suatu Risiko akan terjadi. Pengukurannya bisa menggunakan pendekatan statistik (probability), frekuensi kejadian persatuan waktu (hari, minggu, bulan, tahun) , atau dengan expert judgement

Level Kemungkinan		Persentase Kemungkinan Terjadinya dalam Satu Tahun	Jumlah Frekuensi Kemungkinan Terjadinya dalam Satu Tahun
1	Hampir Tidak Terjadi	X≤5%	X < 2 kali
2	Jarang Terjadi	5%<X≤10%	2 ≤ X ≤ 5 kali
3	Kadang-Kadang Terjadi	10%<X≤20%	6 ≤ X ≤ 9 kali
4	Sering Terjadi	20%<X≤50%	10 ≤ X ≤ 12 kali
5	Hampir Pasti Terjadi	X>50%	> 12 kali

Level Dampak Terjadinya Risiko

Dampak dan probabilitas risiko-risiko ini ditentukan karena berkaitan dengan Keamanan Informasi (CIA). Berdasarkan kriteria penerimaan risiko organisasi, yang merupakan fungsi dari selera terhadap risiko organisasi, organisasi menentukan pendekatan untuk menangani risiko ini.

Nilai	Tingkat Dampak
1	Tidak Signifikan
2	Kurang Signifikan
3	Cukup Signifikan
4	Signifikasn
5	Sangat Signifikan

Kriteria Dampak Risiko

Area Dampak	Level Dampak				
	1	2	3	4	5
	Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Finansial	Tidak terdapat kerugian finansial	terdapat kerugian/biaya yang harus dikeluarkan hingga Rp. 50.000.000,-	terdapat kerugian/biaya yang harus dikeluarkan Rp. 50.000.000,- hingga Rp. 250.000.000,-	terdapat kerugian/biaya yang harus dikeluarkan Rp. 250.000.000,- Rp. 500.000.000,-	terdapat kerugian/biaya yang harus dikeluarkan lebih dari Rp. 500.000.000,-
Reputasi	Terdapat pemberitaan negatif namun tidak mengakibat penurunan kepercayaan	Terdapat pemberitaan negatif yang dapat mempengaruhi tingkat kepercayaan *stakeholder*	terdapat pemberitaan negatif yang terus menurunkan kepercayaan *stakeholder*	hilangnya kepercayaan *stakeholder*	Stakeholder sama sekali tidak percaya
Kinerja	Tidak Menimbulkan penurunan kinerja	Penurunan kinerja sampai 30%	Penurunan kinerja sampai 50%	Penurunan kinerja sampai 70%	Penurunan kinerja sampai 90%
Operasional dan Aset TIK	Terdapat gangguan namun tidak mengakibatkan proses bisnis teraganggu	terdapat gangguan yang menyebabkan 1 mata rantai proses bisnis terganggu	terdapat gangguan yang menyebabkan lebih dari 1 mata rantai proses bisnis terganggu	terdapat gangguan yang menyebabkan seluruh proses bisnis terganggu	terjadi kelumpuhan pada proses bisnis
Hukum dan Regulasi	Tidak Menimbulkan dampak hukum	Menimbulkan dampak hukum kategori ringan	menimbulkan dampak hukum kategori sedang	menimbulkan dampak hukum kategori berat	Menimbulkan kasus Hukum Tindak pidana
Sumber Daya Manusia	Seluruh SDM telah sesuai dengan kebutuhan dan pengembangan kapasitas SDM	Sebagaian Besar / 90% SDM telah sesuai dengan kebutuhan dan pengembangan kapasitas SDM	sebagian kecil / 60% SDM telah sesuai dengan kebutuhan dan pengembangan kapasitas SDM	SDM belum sesuai / 30% dengan kebutuhan dan pengembangan kapasitas SDM	SDM tidak sesuai dengan kebutuhan dan pengembangan kapasitas SDM
Layanan Organisasi	Menimbulkan penundaan layanan organisasi maksimal 24 jam	Menimbulkan penundaan layanan organisasi maksimal 2 x 24 jam	Menimbulkan penundaan layanan organisasi maksimal 3 x 24 jam	Menimbulkan penundaan layanan organisasi maksimal 5 x 24 jam	Menimbulkan penundaan layanan organisasi lebih dari 5 x 24 jam

MATRIKS ANALISIS RISIKO & LEVEL RISIKO

Nilai Risiko

Nilai Risiko merupakan kombinasi antara tingkat kemungkinan terjadinya risiko dan tingkat dampak yang direpresentasikan dengan angka , yang dirumuskan sebagai berikut :

Nilai Risiko = Level Kemungkinan x Level Dampak

Nilai resiko selanjutnya dikelompokkan dalam rentang nilai tertentu untuk memudahkan saat dilakukan seleksi prioritas penanganan risiko

Matriks Analisis Risiko

Matriks Analisis Risiko			Level Dampak				
			1	2	3	4	5
5x5			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Level Kemungkinan	5	Hampir Pasti Terjadi	9	15	18	23	25
	4	Sering Terjadi	6	12	16	19	24
	3	Kadang-Kadang Terjadi	4	10	14	17	22
	2	Jarang Terjadi	2	7	11	13	21
	1	Hampir Tidak Terjadi	1	3	5	8	20

Level Risiko

Level Risiko SPBE

Level Risiko	Rentang Besaran Risiko	Simbol Warna
Sangat Rendah	1 - 5	Biru
Rendah	6 - 10	Hijau
Sedang	11 – 15	Kuning
Tinggi	16 – 20	Jingga
Sangat Tinggi	21 - 25	Merah

Rentang Nilai Risiko	Pernyataan Rentang Nilai Risiko	Simbol Warna	Tindakan yang diambil
1 - 5	Sangat Rendah	Biru	Tidak diperlukan tindakan
6 - 10	Rendah	Hijau	Diambil tindakan jika diperlukan
11 – 15	Sedang	Kuning	Diambil tindakan jika sumber daya tersedia
16 – 20	Tinggi	Jingga	Diperlukan tindakan untuk mengelola risiko
21 - 25	Sangat Tinggi	Merah	Diperlukan tindakan segera untuk mengelola risiko

Matriks Analisis Risiko Versi 31000 (Intermezzo)

Matriks Analisis Risiko			Level Dampak				
			1	2	3	4	5
			Tidak Signifikan	Kecil	Sedang	Besar	Katastrope
Level Kemungkinan	5	Hampir Pasti terjadi	5	10	15	20	25
	4	Sering Terjadi	4	8	12	16	20
	3	Kadang Terjadi	3	6	9	12	15
	2	Jarang Terjadi	2	4	6	8	10
	1	Hampir Tidak terjadi	1	2	3	4	5

Rendah (Hijau), Menengah (Kuning), Tinggi (Orange), Sangat Tinggi (Merah)

Selera Risiko

Selera Risiko bertujuan untuk memberikan acuan dalam penentuan ambang batas minimum terhadap Besaran Risiko yang harus ditangani untuk setiap Kategori Risiko baik Risiko Positif maupun Risiko Negatif. Penentuan Selera Risiko ini dapat disesuaikan dengan kompleksitas Risiko serta konteks internal dan eksternal masing-masing Instansi.

No	Kategori Risiko	Besaran Risiko Minimum Yang ditangani	
		Risiko Positif	Risiko Negatif
1	Peta Rencana	x	16
2	Proyek Pembangunan/Pengembangan Sistem	x	20
3	Data dan Informasi	x	10
4	Infrastruktur	x	16
5	Keamanan	x	16
6	Keamanan	x	16
7	SDM	x	...

Risk Register

Pengisian kolom awal pada saat memulai identifikasi risiko, terdiri dari :

1. **Jenis Risiko**, Jenis Risiko terbagi menjadi Risiko positif dan Risiko negatif. Dalam melakukan identifikasi Risiko, Risiko dituliskan ke dalam masing-masing jenis Risiko SPBE.
2. **Kejadian (Pernyataan Risiko),** Kejadian dapat diidentifikasi dari terjadinya suatu peristiwa yang menimbulkan Risiko SPBE yang diperoleh dari riwayat peristiwa dan/atau prediksi terjadinya peristiwa di masa yang akan datang.
3. **Jenis Ancaman**, Jenis Ancaman mengacu kepada probabilitas ancaman keamanan informasi yang terganggu dari bagian Confidentiality, Integrity, atau Availability yang diidentifikasi dari pernyataan risiko
4. **Penyebab**, Penyebab dapat diidentifikasi dari akar masalah yang menjadi pemicu munculnya Risiko. Penyebab dapat berasal dari lingkungan internal maupun eksternal Instansi Pusat dan Pemerintah Daerah. Identifikasi penyebab akan membantu menemukan tindakan yang tepat untuk menangani Risiko.
5. **Kategori,** Penentuan Kategori Risiko didasarkan pada penyebab dari munculnya Risiko.
6. **Dampak,** Dampak dapat diidentifikasi dari pengaruh atau akibat yang timbul dari Risiko SPBE.
7. **Area Dampak**, Penentuan Area Dampak Risiko didasarkan pada dampak yang telah teridentifikasi.

Risk Register

Identifikasi Risiko						
Jenis Risiko	**Kejadian (Pernyataan)**	**Jenis Ancaman (C/I/A)**	**Penyebab**	**Kategori**	**Dampak**	**Dampak Area**
Positif						
Negatif	Aplikasi ter-deface	Availability	Adanya celah pada pemrograman aplikasi yang mudah ditembus pihak luar	Keamanan	Operasional organisasi terganggu	Kinerja

Risk Register

Pengisian kolom selanjutnya yaitu kolom analisis risiko, terdiri dari :

a. Sistem Pengendalian
   - Sistem pengendalian internal mencakup perangkat manajemen yang dapat menurunkan/meningkatkan level Risiko dalam rangka pencapaian sasaran
   - Sistem pengendalian internal dapat berupa *Standard Operating Procedure* (SOP), pengawasan melekat, reviu berjenjang, regulasi, dan pemantauan rutin yang dilaksanakan terkait Risiko tersebut.

b. Level Kemungkinan

c. Level Dampak

d. Besaran Risiko (Nilai Risiko) dan Level Risiko

Risk Register

Analisis Risiko				
Sistem Pengendalian	Kemungkinan	Dampak	Nilai Risiko	Level Risiko
	Level	Level		
Penyusunan prosedur Penetration Test	5	4	23	Sangat Tinggi

Risk Register

Pengisian kolom selanjutnya yaitu kolom rencana penanganan risiko. Terdiri dari Opsi Penanganan Risiko, Rencana Aksi Penanganan Risiko, Keluaran, Jadwal Implementasi, dan Penanggung Jawab. Adapun Opsi Penanganan Risiko (Negatif) terdiri dari :

- **Eskalasi Risiko**: Eskalasi risiko dipilih jika **Risiko berada di luar atau melampaui wewenang**. Opsi ini dilakukan dengan **memindahkan tanggung jawab** penanganan Risiko ke unit kerja yang lebih tinggi.
- **Mitigasi Risiko**: Mitigasi risiko dilakukan dengan cara **mengurangi level** kemungkinan dan/atau level dampak dari Risiko
- **Transfer Risiko**: Transfer risiko dipilih jika terdapat kekurangan sumber daya untuk mengelola Risiko. Opsi ini dilakukan dengan cara mengalihkan kepemilikan risiko kepada pihak lain untuk melakukan pengelolaan dan pertanggungjawaban terhadap Risiko.
- **Penghindaran Risiko**: Penghindaran risiko dilakukan dengan mengubah perencanaan, penganggaran, program, dan kegiatan, atau aspek lainnya untuk mencapai sasaran SPBE.
- **Penerimaan Risiko**: Opsi ini dipilih jika biaya dan usaha penanganan lebih tinggi diandingkan manfaat yang di dapat, Tindakan yang di ambil adalah membiarkan risiko tersebut terjadi apadanya

Risk Register

Rencana Penanganan Risiko				
Opsi Penanganan	**Rencana Aksi Penanganan Risiko**	**Keluaran**	**Jadwal Implementasi**	**Penanggung Jawab**
Mitigasi	Melakukan Penetration Test dan mencatat hasil Penetration Test	Laporan hasil Penetration Test	Pada saat perbaikan	Bidang Infrastruktur, Keamanan dan Informasi

Risk Register

ID	Identifikasi Risiko							Analisis Risiko					Rencana Penanganan Risiko				
	Jenis Risiko	Kejadian (Pernyataan)	Jenis Ancaman (C/I/A)	Penyebab	Kategori	Dampak	Dampak Area	Sistem Pengendalian	Kemungkinan	Dampak	Nilai Risiko	Level Risiko	Opsi Penanganan Risiko	Rencana Aksi Penanganan Risiko	Keluaran	Jadwal Implementasi	Penanggung Jawab
									Level	Level							
1	Positif																
1	Negatif	Aplikasi ter-deface	Availability	Adanya celah pada pemrograman aplikasi yang mudah ditembus pihak luar	Keamanan	Operasional organisasi terganggu	Kinerja	Penyusunan prosedur Penetration Test	5	4	23	Sangat Tinggi	Mitigasi	Melakukan Penetration Test dan mencatat hasil Penetration Test	Laporan hasil Penetration Test	Pada saat perbaikan	Bidang Infrastruktur, Keamanan dan Informasi

***Hanya Contoh**

Klausul 6.1.3 Penanganan risiko keamanan informasi

Organisasi harus menetapkan dan menerapkan proses penanganan risiko keamanan informasi untuk:

Informasi terdokumentasi dipelihara

Statement of Applicability (SOA)

Dokumentasi Analisis Kontrol Implementasi SMKI

Pernyataan Kontrol terhadap Annex A SNI ISO/IEC 27001:2022

4 Domain dan 93 Kontrol Keamanan Informasi

Statement of Applicability (SOA)

Pernyataan Pemberlakuan

Versi 1.0
Tanggal 03/10/2022
Ruang Lingkup SMKI

ISO/IEC 27001:2013 Statement of Applicability				Apakah kontrol bisa diaplikasikan? (YA / TIDAK)	Alasan / Keterangan pemilihan kendali annex	Referensi dokumen/bukti dukung (Kebijakan, prosedur, formulir)	Keterangan Tambahan (jika Ada)
Area	**Section**	**Control**	**Deskripsi Kontrol**				
A.5 Kebijakan keamanan informasi							
	A.5.1 Arahan manajemen untuk keamanan informasi	A.5.1.1 Kebijakan untuk keamanan informasi	Kendali Seperangkat kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak luar yang terkait.				
		A.5.1.2 Reviu kebijakan keamanan informasi	Kendali Kebijakan untuk keamanan informasi harus direviu pada interval waktu terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan dan keefektifan yang berkelanjutan				
A.6 Organisasi keamanan informasi							
	A.6.1 Organisasi internal	A.6.1.1 Peran dan tanggung jawab keamanan informasi	Kendali Semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan.				
		A.6.1.2 Pemisahan tugas	Kendali Tugas dan area tanggung jawab yang bertentangan harus dipisahkan (dijabat oleh personel yang berbeda) untuk mengurangi kemungkinan dari modifikasi yang tidak sah atau tidak sengaja atau penyalahgunaan aset organisasi.				
		A.6.1.3 Hubungan dengan pihak berwenang	Kendali Hubungan baik dengan pihak berwenang terkait harus dipelihara.				

Klausul 6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

Organisasi harus menetapkan sasaran keamanan informasi pada fungsi dan level yang relevan. Sasaran keamanan informasi harus:

a) konsisten dengan kebijakan keamanan informasi;
b) dapat diukur (jika dapat dipraktikkan);
c) mempertimbangkan persyaratan keamanan informasi yang dapat diaplikasikan, dan hasil dari asesmen risiko dan penanganan risiko;
d) termonitorkan;
e) terkomunikasikan;
f) termutakhirkan dengan tepat;
g) tersedia sebagai informasi terdokumentasi.

Organisasi harus menyimpan informasi terdokumentasi mengenai sasaran keamanan informasi.

Klausul 6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

Ketika merencanakan bagaimana mencapai sasaran keamanan informasinya, organisasi harus menentukan:

Contoh sasaran SMKI: Dilakukan pencadangan data (*backup*) secara rutin minimum 1 kali seminggu.

Informasi terdokumentasi dipelihara

Contoh Sasaran SMKI

Sasaran SMKI
- Daftar inventaris sistem aplikasi diperbaharui setiap tahunnya - Dilakukan pencadangan basis data (*Back up data base)* secara rutin sesuai periode yang ditetapkan - Dilakukan pembaharuan anti virus secara rutin sesuai periode yang ditetapkan - Tingkat kegagalan sistem aplikasi maksimal 5% setiap tahunnya
- Daftar inventaris aset server dan jaringan diperbaharui setiap tahunnya - Serangan dari luar teridentifikasi setiap tahunnya - Tingkat kegagalan server maksimal 5% setiap tahunnya
- Dilakukan perawatan dan monitoring kondisi komputer pribadi dan alat pendukungnya secara berkala - Daftar inventaris aset komputer pribadi dan alat pendukungnya diperbaharui setiap tahunnya

6.3 Perencanaan perubahan

Ketika organisasi menentukan kebutuhan perubahan atas sistem manajemen keamanan informasi, perubahan tersebut harus dilakukan dengan cara yang terencana.

Klausul 7 Dukungan

Klausul 7.1 Sumber Daya

"Organisasi harus menentukan dan menyediakan **sumber daya** yang dibutuhkan untuk penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI".

- Sumber Daya Manusia
- Sumber Daya Teknis
- Sumber Daya Keuangan

Sumber daya manusia, misalnya manajemen puncak, personel yang terlibat dalam penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI;

Sumber daya teknis, misalnya sistem dan infrastruktur yang mendukung implementasi SMKI;

Sumber daya keuangan, termasuk dana untuk proyek dan dana untuk pengoperasian penerapan SMKI.

Klausul 7.2 Kompetensi

Organisasi **Harus** :

a. menentukan kompetensi yang diperlukan untuk personel yang melakukan pekerjaan di bawah kendali organisasi yang mempengaruhi kinerja keamanan informasi organisasi;

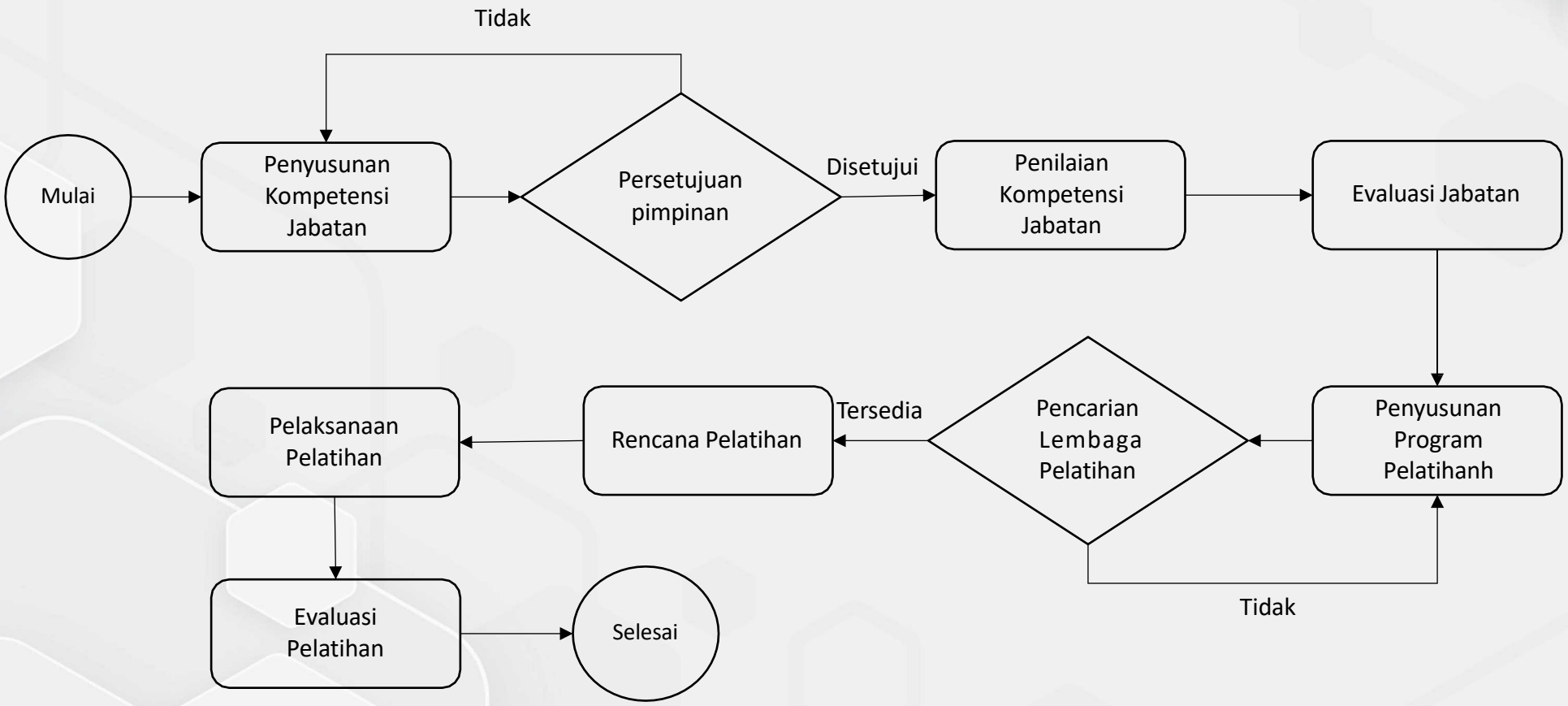
b. memastikan bahwa personel ini kompeten berdasarkan pendidikan, pelatihan, atau pengalaman yang sesuai;

c. apabila memungkinkan, mengambil tindakan untuk memperoleh kompetensi yang diperlukan, dan mengevaluasi efektivitas tindakan yang diambil; dan

d. menyimpan informasi terdokumentasi yang sesuai sebagai alat bukti kompetensi

CATATAN : Tindakan yang bisa diterapkan dapat meliputi, misal: penyediaan pelatihan, bimbingan, atau penugasan kembali temadap karyawan yang ada; atau merekrut atau mengontrak personel yang kompeten

Flow Pengelolaan Kompetensi



Klausul 7.2 Kompetensi

Peran/ Jabatan	Deskripsi Pekerjaan	Persyaratan Komptensi		
		Pendidikan	Pengalaman Kerja	Pelatihan
Web Programmer	Membuat aplikasi menggunakan framework PHP ..	S1 Teknologi Informasi, …	Membuat aplikasi XYZ di PT. ABC	Framework PHP version ..

Klausul 7.3 Kepedulian

Personel yang bekerja di bawah kendali organisasi harus peduli terhadap:

a) kebijakan keamanan informasi;

b)kontribusinya terhadap efektivitas SMKI, termasuk manfaat peningkatan kinerja keamanan informasi; dan

c) implikasi dari ketidaksesuaian dengan persyaratan SMKI.

Annex A.7.2.2

Sosialisasi

Poster/Media cetak

Socmed

Organisasi **harus** menentukan kebutuhan berkomunikasi internal dan eksternal yang relevan dengan SMKI yang mencakup:

- apa yang akan dikomunikasikan ?
- kapan berkomunikasi ?
- dengan siapa berkomunikasi ?
- proses yang dipengaruhi oleh komunikasi tersebut
- siapa yang harus mengomunikasikan

Klausul 7.4 Komunikasi

No	Materi Komunikasi	Periode Komunikasi	Target Penerima	Media Komunikasi	**PIC**
1	Sasaran SMKI	Tiap Tahun	Semua Pegawai	Teleconference	Koordinator SMKI

Klausul 7.5 Informasi Terdokumentasi

7.5.1 Umum

Organisasi SMKI harus mencakup:

a) informasi terdokumentasi yang disyaratkan oleh Standar ini; dan

b)informasi terdokumentasi yang ditentukan oleh organisasi, sesuai yang diperlukan untuk efektivitas SMKI.

CATATAN cakupan informasi terdokumentasi untuk SMKI dapat berbeda antara satu organisasi dengan organisasi yang lain karena:

1) ukuran organisasi dan jenis kegiatan, proses, produk dan layanannya;
2) kompleksitas proses dan interaksinya; dan
3) kompetensi personelnya.

ISO 10013:2021

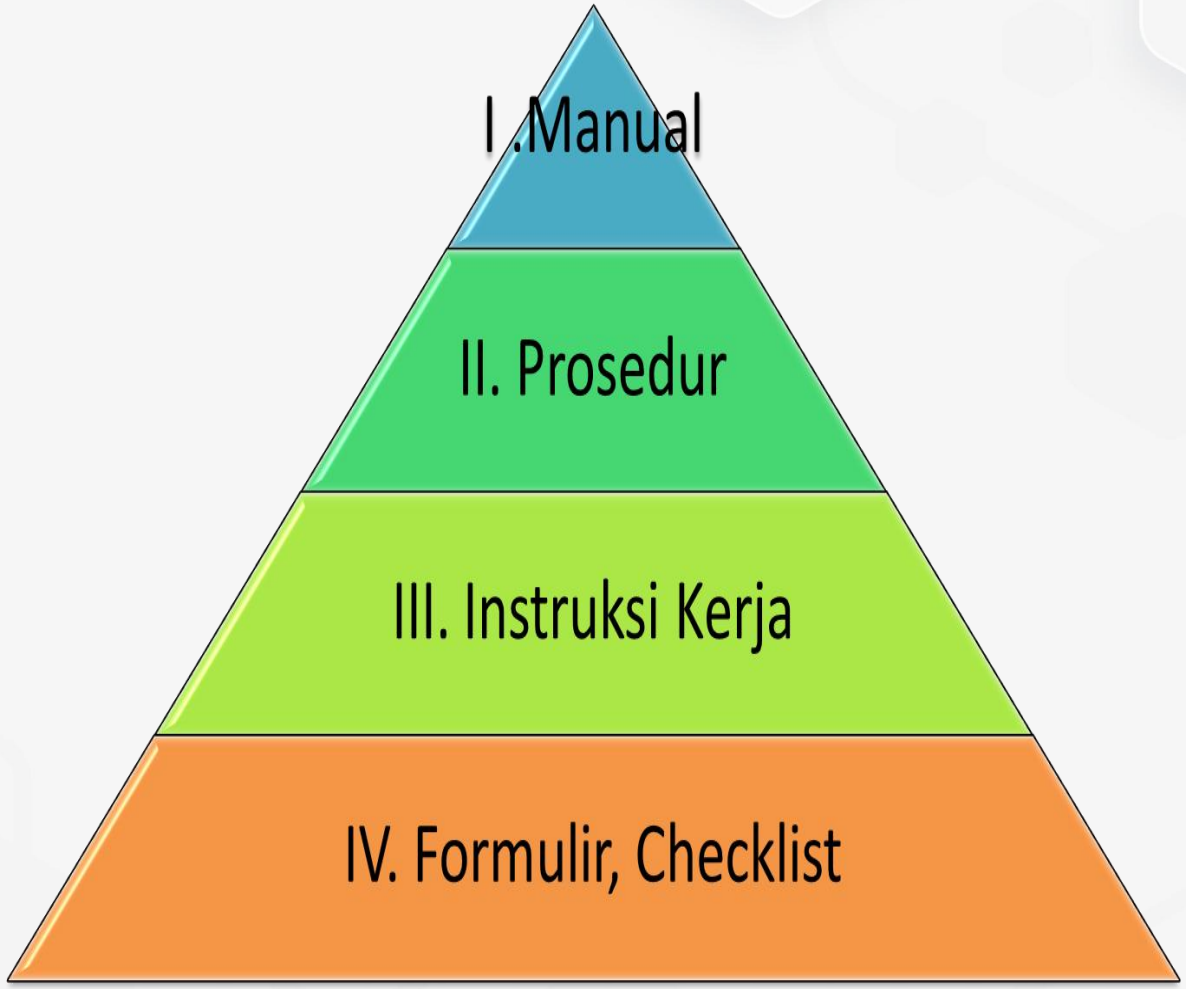
Klausul 7.5 Informasi Terdokumentasi

komitmen dan kebijakan , peraturan perundangan Dll

Rangakain Kegiatan SMKI, Uraian Kebijakan dll

Bagaimana/Cara/Langkah2 seseorang melaksanakan tugas

Bukti, Atau rekaman dokumen



Klausul 7.5 Informasi Terdokumentasi

7.5.2 Membuat dan memperbarui

Ketika membuat dan memperbarui informasi terdokumentasi organisasi **harus** memastikan kecukupan hal-hal berikut ini:

a) identifikasi dan deskripsi (misal judul, tanggal, penulis, atau nomor referensi);

b) format (misal bahasa, versi perangkat lunak, grafis) dan media (misal kertas, elektronik); dan

c) reviu dan persetujuan untuk kesesuaian dan kecukupan.

Klausul 7.5 Informasi Terdokumentasi

7.5.3 Pengendalian informasi terdokumentasi

Informasi terdokumentasi yang dibutuhkan oleh SMKI dan Standar ini harus dikendalikan untuk memastikan:

- informasi terdokumentasi tersedia dan cocok untuk digunakan, di mana dan kapan saja diperlukan; dan
- informasi terdokumentasi cukup terlindungi (misal dari terungkapnya kerahasiaan, penyalahgunaan, atau hilangnya integritas).

Klausul 7.5 Informasi Terdokumentasi

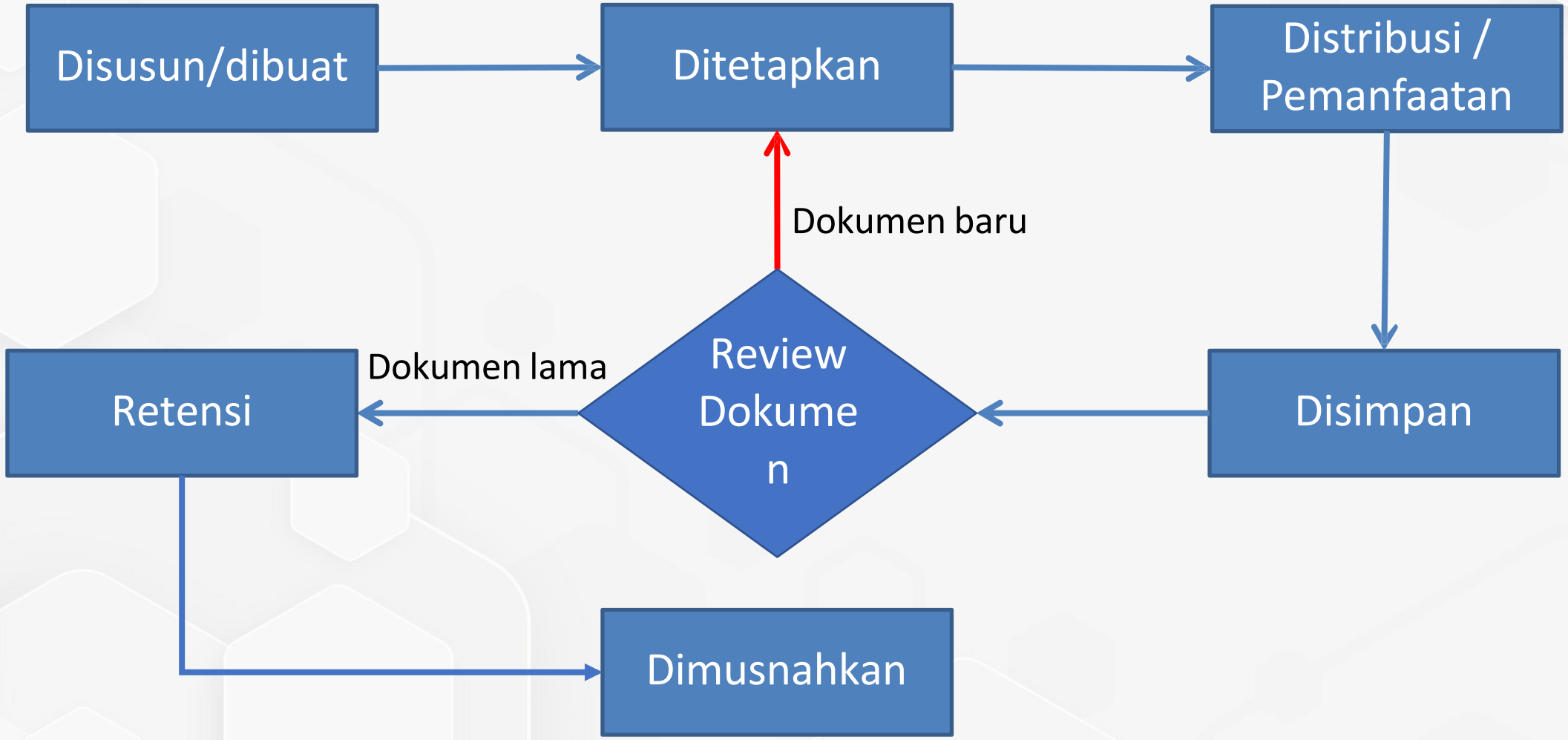
Untuk pengendalian informasi terdokumentasi, organisasi harus menangani kegiatan- kegiatan berikut, jika dapat diterapkan:

- distribusi, akses, pengambilan dan penggunaan;
- penyimpanan dan pemeliharaan, termasuk pemeliharaan keterbacaan *(legibility)*;
- pengendalian perubahan, misal pengendalian versi *(version control)*; dan
- retensi (*retention*) dan disposisi *(disposition)*.

Informasi terdokumentasi yang bersumber dari luar, yang menurut organisasi diperlukan untuk perencanaan dan operasi SMKI, harus diidentifikasi kesesuaiannya dan dikendalikan.

CATATAN Akses mencakup keputusan terkait izin dan kewenangan untuk melihat informasi terdokumentasi saja, atau melihat dan mengubah informasi terdokumentasi, dll.

Siklus dokumen



Tugas Klausul 6

1. Buatlah identifikasi Level Kemungkinan & Kriteria Dampak Risiko
2. Buatlah Dokumen Risk Register

Tugas Klausul 7

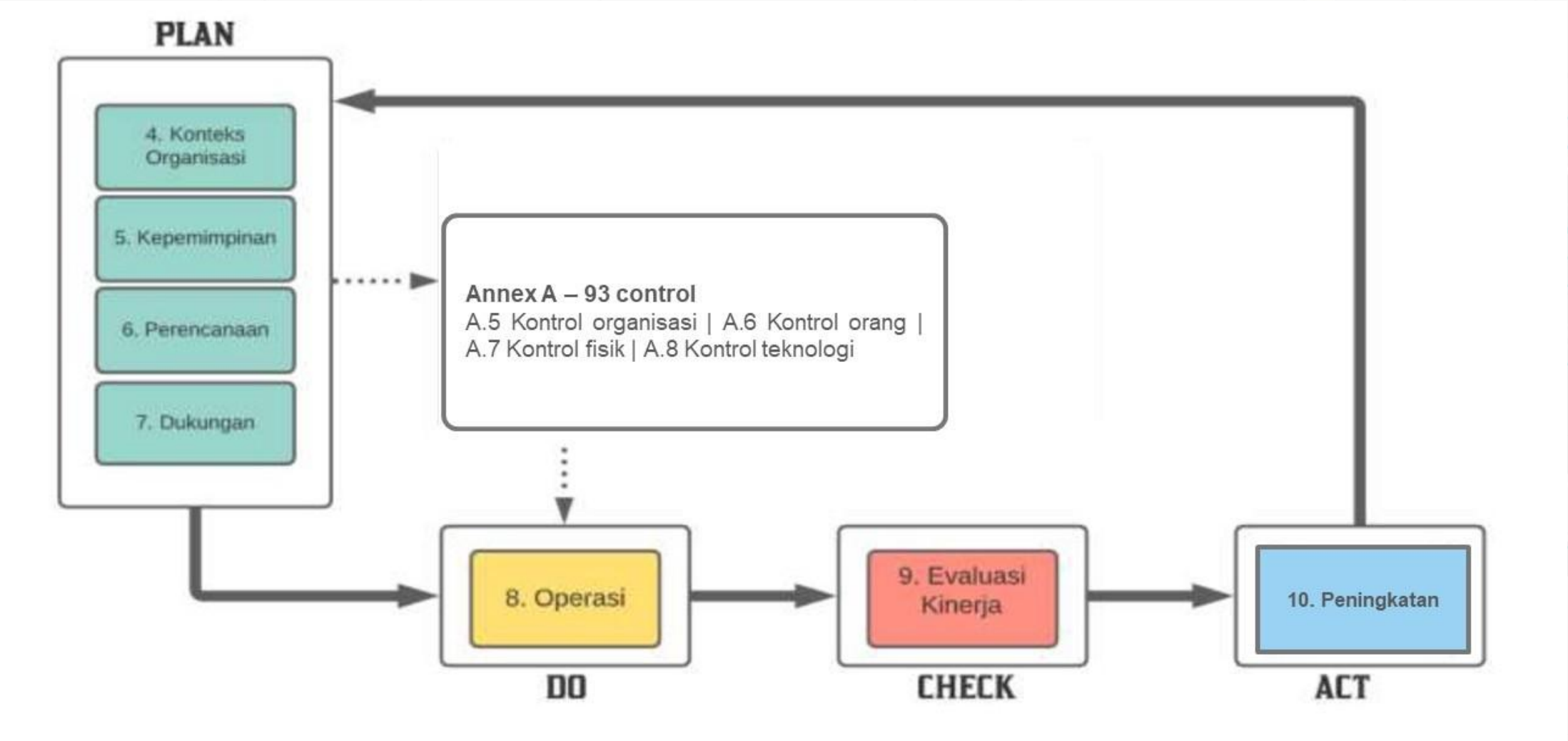
1. mengidentifikasi kebutuhan kompetensi untuk keamanan informasi di masing- masing instansi (7.2)
2. Mengidentifikasi bentuk komunikasi dan kepedulian keamanan informasi di masing-masing instansi (7.4)

TERIMA KASIH

Sistem Manajemen Keamanan Informasi SNI ISO/IEC 27001:2022

Pertemuan 5 - Klausul 8 Operasi

Siklus PDCA SNI ISO/IEC 27001:2022



Klausul 8.1 Perencanaan dan pengontrolan operasional

- Organisasi harus merencanakan, mengimplementasi dan mengontrol proses yang dibutuhkan untuk memenuhi persyaratan, dan untuk mengimplementasikan tindakan yang ditentukan dalam Pasal 6, dengan:
- — menetapkan kriteria untuk proses;
  — mengimplementasikan kontrol atas proses berdasarkan kriteria.
- Organisasi harus menyimpan informasi terdokumentasi sejauh yang diperlukan untuk memiliki keyakinan bahwa proses telah dilakukan seperti yang direncanakan.
- Organisasi harus mengontrol perubahan yang direncanakan dan mereviu konsekuensi dari perubahan yang tidak diinginkan, mengambil tindakan untuk memitigasi efek buruk, sebagaimana diperlukan.
- Organisasi harus memastikan bahwa proses, produk, atau layanan yang disediakan secara eksternal yang relevan terhadap sistem manajemen keamanan informasi telah dikontrol.

Klausul 8.2 Asesmen risiko keamanan informasi

- Organisasi harus melakukan asesmen risiko keamanan informasi pada interval terencana atau ketika perubahan signifikan diusulkan atau terjadi, dengan mempertimbangkan kriteria yang ditetapkan dalam 6.1.2 a).
- Organisasi harus menyimpan informasi terdokumentasi dari hasil asesmen risiko keamanan informasi.

Klausul 8.3 Penanganan risiko keamanan informasi

- Organisasi harus mengimplementasikan rencana penanganan risiko keamanan informasi. Organisasi harus menyimpan informasi terdokumentasi hasil penanganan risiko keamanan informasi.

Operasi sistem manajemen keamanan informasi dilakukan melalui penerapan kontrol keamanan informasi yang mengacu kepada Lampiran A (Annex A) SNI ISO/IEC 27001:2022 yang bersifat normatif.

Lampiran/ Annex A (normatif)

- SNI ISO/IEC 27001:2022
- Terdiri dari 4 kategori dengan 93 kontrol

A: 5 Kontrol organisasi [37]

A: 6 Kontrol orang [8]

A: 7 Kontrol fisik [14]

A: 8 Kontrol teknologi [34]

93 kontrol Annex A di versi 2022

5. Kontrol Organisasi

5.1 Kebijakan keamanan informasi
5.2 Peran dan tanggung jawab keamanan informasi
5.3 Segregasi tugas
5.4 Tanggung jawab manajemen
5.5 Kontak dengan otoritas
5.6 Kontak dengan kelompok kepentingan khusus
5.7 Intelijen ancaman
5.8 Keamanan informasi dalam manajemen proyek
5.9 Inventarisasi informasi dan aset terkait lainnya
5.10 Penggunaan yang akseptabel dari informasi dan aset terkait lainnya
5.11 Pengembalian aset
5.12 Klasifikasi informasi
5.13 Pelabelan informasi
5.14 Transfer informasi
5.15 Kontrol akses
5.16 Manajemen identitas
5.17 Informasi autentikasi
5.18 Hak akses
5.19 Keamanan informasi dalam hubungan pemasok
5.20 Menangani keamanan informasi dalam perjanjian pemasok
5.21 Memanajemeni keamanan informasi dalam rantai pasokan TIK
5.22 Pemonitoran, reviu, dan manajemen perubahan layanan pemasok
5.23 Keamanan informasi untuk penggunaan layanan cloud
5.24 Perencanaan dan persiapan manajemen insiden keamanan informasi
5.25 Asesmen dan keputusan tentang peristiwa keamanan informasi
5.26 Respons terhadap insiden keamanan informasi
5.27 Belajar dari insiden keamanan informasi
5.28 Pengumpulan bukti
5.29 Keamanan informasi selama disrupsi
5.30 Kesiapan TIK untuk kontinuitas bisnis
5.31 Persyaratan legal, statutori, regulatori, dan kontraktual
5.32 Hak kekayaan intelektual
5.33 Proteksi rekaman
5.34 Privasi dan proteksi personal identifiable information (PII)
5.35 Reviu independen terhadap keamanan informasi
5.36 Kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi
5.37 Prosedur operasi terdokumentasi

6. Kontrol Orang

6.1 Skrining
6.2 Syarat dan ketentuan ketenagakerjaan
6.3 Kesadaran, pendidikan dan pelatihan keamanan informasi
6.4 Proses kedisiplinan
6.5 Tanggung jawab setelah terminasi atau perubahan pekerjaan
6.6 Perjanjian konfidensialitas atau nirungkap
6.7 Telekarya (Remote working)
6.8 Pelaporan peristiwa keamanan informasi

7. Kontrol Fisik

7.1 Perimeter keamanan fisik
7.2 Entri fisik
7.3 Mengamankan kantor, ruangan, dan fasilitas
7.4 Pemonitoran keamanan fisik
7.5 Memproteksi dari ancaman fisik dan lingkungan
7.6 Bekerja di area yang aman
7.7 Meja bersih dan layar bersih
7.8 Penempatan dan proteksi peralatan
7.9 Keamanan aset di luar lokasi
7.10 Media penyimpanan
7.11 Utilitas pendukung
7.12 Keamanan perkabelan
7.13 Pemeliharaan peralatan
7.14 Pemusnahan atau penggunaan kembali peralatan dengan aman

8. Kontrol Teknologi

8.1 Perangkat titik akhir pengguna
8.2 Hak akses privilese
8.3 Pembatasan akses informasi
8.4 Akses ke kode sumber
8.5 Autentikasi aman
8.6 Manajemen kapasitas
8.7 Proteksi terhadap perangkat perusak
8.8 Manajemen kerentanan teknis
8.9 Manajemen konfigurasi
8.10 Penghapusan informasi
8.11 Penyamaran (masking) data
8.12 Pencegahan kebocoran data
8.13 Pencadangan informasi
8.14 Redundansi fasilitas pemrosesan informasi
8.15 Membuat log
8.16 Pemonitoran aktivitas
8.17 Sinkronisasi jam
8.18 Penggunaan program utilitas privilese
8.19 Instalasi perangkat lunak pada sistem operasional
8.20 Keamanan jaringan
8.21 Keamanan layanan jaringan
8.22 Segregasi jaringan
8.23 Pemfilteran web
8.24 Penggunaan kriptografi
8.25 Siklus hidup pengembangan yang aman
8.26 Persyaratan keamanan aplikasi
8.27 Prinsip-prinsip arsitektur dan rekayasa sistem yang aman
8.28 Pengkodean yang aman
8.29 Pengujian keamanan dalam pengembangan dan penerimaan
8.30 Pengembangan yang dialihdayakan
8.31 Pemisahan lingkungan pengembangan, pengujian, dan produksi
8.32 Manajemen perubahan
8.33 Informasi uji
8.34 Proteksi sistem informasi selama pengujian audit

A.5. Kontrol Organisasi [37]

1.Kebijakan Keamanan Organisasi

Kontrol

Kebijakan keamanan infoímasi dan kebijakan topik spesifik haíus didefinisikan, disetujui oleh manajemen, dipublikasikan, dikomunikasikan, dan diakui oleh peísonel teíkait dan pihak beíkepentingan teíkait, dan diíeviu secaía beíkala sesuai íencana dan jika teíjadi peíubahan yang signifikan.

2.Peran dan tanggung jawab keamanan informasi

Kontrol

Peían dan tanggung jawab keamanan infoímasi haíus didefinisikan dan dialokasikan sesuai dengan kebutuhan oíganisasi.

A.5. Kontrol Organisasi

A.5.3 Segíegasi tugas

Kontíol

l'u gas yang beítentangan dan bidang tanggung jawab yang beítentangan haíus dipisahkan.

A.5.4 l'anggung jawab manajemen

Kontíol

Manajemen haíus mensyaíatkan semua peísonel untuk meneíapkan keamanan infoímasi sesuai dengan kebijakan keamanan infoímasi, kebijakan topik spesifik, dan píoseduí oíganisasi yang ditetapkan.

A.5. Kontrol Organisasi

5.Kontak dengan otoíitas

Kontíol

Oíganisasi haíus menjalin dan memelihaía kontak dengan otoíitas teíkait.

6.Kontak dengan kelompok kepentingan khusus

Kontíol

Oíganisasi haíus menjalin dan memelihaía kontak dengan kelompok kepentingan spesial atau foíum keamanan spesialis lainnya dan asosiasi píofesional.

7.Intelijen ancaman

Kontíol

Infoímasi yang beíkaitan dengan ancaman keamanan infoímasi haíus dikumpulkan dan dianalisis untuk menghasilkan intelijen ancaman.

.

A.5. Kontrol Organisasi

8.Keamanan infoímasi dalam manajemen píoyek

Kontíol

Keamanan infoímasi haíus diintegíasikan ke dalam manajemen píoyek.

9.Inventaíisasi infoímasi dan aset teíkait lainnya

Kontíol

Suatu inventoíi infoímasi dan aset teíkait lainnya, teímasuk pemiliknya, haíus dikembangkan dan dipelihaía.

10.Penggunaan yang akseptabel daíi infoímasi dan aset teíkait lainnya Kontíol

Atuían penggunaan yang akseptabel dan píoseduí untuk menangani infoímasi dan aset teíkait lainnya haíus diidentifikasi, didokumentasikan, dan diimplementasikan.

A.5. Kontrol Organisasi

11.Pengembalian aset

Kontrol

Personel dan pihak berkepentingan lainnya yang tepat harus mengembalikan semua aset organisasi yang dalam kepemilikan mereka setelah perubahan atau pemutusan hubungan kerja, kontrak, atau perjanjian mereka.

12.Klasifikasi informasi

Kontrol

Informasi harus diklasifikasikan sesuai dengan kebutuhan keamanan informasi organisasi berdasarkan konfidensialitas, integritas, availabilitas, dan persyaratan pihak berkepentingan yang relevan.

A.5. Kontrol Organisasi

13.Pelabelan informasi

Kontrol

Seperangkat prosedur yang tepat untuk pelabelan informasi harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.

14.Transfer informasi

Kontrol

Aturan, prosedur, atau perjanjian transfer informasi harus diterapkan untuk semua tipe.

15.Kontrol akses

Kontrol

Aturan untuk mengontrol akses fisik dan logikal ke informasi dan aset terkait lainnya harus ditetapkan dan diimplementasikan berdasarkan persyaratan bisnis dan keamanan informasi.

A.5. Kontrol Organisasi

16.Manajemen identitas

Kontrol

Siklus hidup penuh dari identitas harus dimanajemeni.

17.Informasi autentikasi

Kontrol

Alokasi dan manajemen informasi autentikasi harus dikontrol dengan proses manajemen, termasuk menasihati personel tentang penanganan informasi autentikasi yang tepat.

A.5.18 Hak akses

Kontrol

Hak akses terhadap informasi dan aset terkait lainnya harus disediakan, direviu, dimodifikasi, dan dipindahkan sesuai dengan kebijakan topik spesifik organisasi dan aturan tentang kontrol akses.

A.5. Kontrol Organisasi

A.5.19 Keamanan informasi dalam hubungan pemasok

Kontrol

Proses dan prosedur harus didefinisikan dan diimplementasikan untuk memanajemeni risiko keamanan informasi yang terkait dengan penggunaan produk atau layanan pemasok.

21.Memanajemeni keamanan informasi dalam rantai pasokan TIK

Kontrol

Proses dan prosedur harus didefinisikan dan diimplementasikan untuk memanajemeni risiko keamanan informasi yang terkait dengan rantai pasokan produk dan layanan TIK.

22.Pemonitoran, reviu, dan manajemen perubahan layanan pemasok

Kontrol

Organisasi harus secara reguler memonitor, mereviu, mengevaluasi, dan memanajemeni perubahan dalam praktik keamanan informasi pemasok dan penyampaian layanan.

A.5. Kontrol Organisasi

23. Keamanan informasi untuk penggunaan layanan cloud

Kontrol

Proses untuk akuisisi, penggunaan, manajemen, dan keluar dari layanan cloud harus ditetapkan sesuai dengan persyaratan keamanan informasi organisasi.

24.Perencanaan dan persiapan manajemen insiden keamanan informasi

Kontrol

Organisasi harus merencanakan dan menyiapkan memanajemeni insiden keamanan informasi dengan mendefinisikan, menetapkan dan mengkomunikasikan proses, peran dan tanggung jawab manajemen insiden keamanan informasi

A.5. Kontrol Organisasi

25.Asesmen dan keputusan tentang peristiwa keamanan informasi

Kontrol

Organisasi harus menilai peristiwa keamanan informasi dan memutuskan apakah peristiwa tersebut akan dikategorikan sebagai insiden keamanan informasi.

26.Respons terhadap insiden keamanan informasi

Kontrol

Insiden keamanan informasi harus direspons sesuai dengan prosedur yang terdokumentasi.

A.5.27 Belajar dari insiden keamanan informasi

Kontrol

Pengetahuan yang diperoleh dari insiden keamanan informasi harus digunakan untuk memperkuat dan meningkatkan kontrol keamanan informasi.

A.5. Kontrol Organisasi

28.Pengumpulan bukti

Kontrol

Organisasi harus menetapkan dan mengimplementasikan prosedur untuk identifikasi, pengumpulan, akuisisi, dan preservasi bukti yang terkait dengan peristiwa keamanan informasi.

29.Keamanan informasi selama disrupsi

Kontrol

Organisasi harus merencanakan bagaimana memelihara keamanan informasi pada level yang tepat selama disrupsi.

30.Kesiapan TIK untuk kontinuitas bisnis

Kontrol

Kesiapan TIK harus direncanakan, diimplementasikan, dipelihara, dan diuji berdasarkan sasaran kontinuitas bisnis dan persyaratan kontinuitas TIK.

A.5. Kontrol Organisasi

31.Persyaratan legal, statutori, regulatori, dan kontraktual

Kontrol

Persyaratan legal, statutori, regulatori, dan kontraktual yang relevan dengan keamanan informasi dan pendekatan organisasi untuk memenuhi persyaratan ini harus diidentifikasi, didokumentasikan, dan diperbarui.

32.Hak kekayaan intelektual

Kontrol

Organisasi harus mengimplementasikan prosedur yang tepat untuk memproteksi hak kekayaan intelektual.

33.Proteksi rekaman

Kontrol

Rekaman harus diproteksi dari kehilangan, perusakan, pemalsuan, akses takterotorisasi, dan rilis takterotorisasi.

A.5. Kontrol Organisasi

34.Privasi dan proteksi personal identifiable information (PII)

Kontrol

Organisasi harus mengidentifikasi dan memenuhi persyaratan mengenai preservasi privasi dan proteksi PII sesuai dengan hukum dan regulasi yang berlaku dan persyaratan kontraktual.

35.Reviu independen terhadap keamanan informasi

Kontrol

Pendekatan organisasi untuk memanajemeni keamanan informasi dan implementasinya termasuk orang, proses, dan teknologi harus direviu secara independen pada interval yang direncanakan, atau ketika perubahan signifikan terjadi.

A.5. Kontrol Organisasi

36.Kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi

Kontrol

Kepatuhan terhadap kebijakan keamanan informasi organisasi, kebijakan topik spesifik, aturan, dan standar harus direviu secara reguler.

37.Prosedur operasi terdokumentasi

Kontrol

Prosedur operasi untuk fasilitas pemrosesan informasi harus didokumentasikan dan tersedia untuk personel yang membutuhkannya.

A.6. Kontrol Orang [8]

A.6.1 Skrining

Kontrol

Pemeriksaan verifikasi latar belakang pada semua kandidat untuk menjadi personel harus dilakukan sebelum bergabung dengan organisasi dan secara berkelanjutan dengan konsiderasi hukum, regulasi, dan etika serta proporsional dengan persyaratan bisnis, klasifikasi informasi yang akan diakses, dan risiko yang dipersepsikan.

A.6.2 Syarat dan ketentuan ketenagakerjaan

Kontrol

Perjanjian kontraktual kerja harus menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi.

A.6. Kontrol Orang [8]

3.Kesadaran, pendidikan dan pelatihan keamanan informasi

Kontrol

Personel organisasi dan pihak terkait yang relevan harus menerima kesadaran keamanan informasi yang tepat, pendidikan dan pelatihan dan pembaruan reguler dari kebijakan keamanan informasi organisasi, kebijakan dan prosedur khusus topik, yang relevan untuk fungsi pekerjaannya.

4.Proses kedisiplinan

Kontrol

Proses disiplin harus disusun dan dikomunikasikan untuk mengambil tindakan terhadap personel dan pihak berkepentingan lain yang relevan yang telah melakukan pelanggaran kebijakan keamanan informasi.

A.6. Kontrol Orang [8]

5.Tanggung jawab setelah terminasi atau perubahan pekerjaan

Kontrol

Tanggung jawab dan tugas keamanan informasi yang tetap berlaku setelah terminasi atau perubahan pekerjaan harus didefinisikan, ditegakkan, dan dikomunikasikan kepada personel terkait dan pihak lain yang berkepentingan.

6.Perjanjian konfidensialitas atau nirungkap

Kontrol

Perjanjian konfidensialitas atau nirungkap yang merefleksikan kebutuhan organisasi untuk proteksi informasi harus diidentifikasi, didokumentasikan, direviu secara regular, dan ditandatangani oleh personel dan pihak terkait lainnya yang relevan.

A.6. Kontrol Orang [8]

7.Telekarya (Remote working)

Kontrol

Langkah keamanan harus diimplementasikan ketika personel bekerja dari jarak jauh untuk memproteksi informasi yang diakses, diproses, atau disimpan di luar premis organisasi.

8.Pelaporan peristiwa keamanan informasi

Kontrol

Organisasi harus menyediakan mekanisme bagi personel untuk melaporkan peristiwa keamanan informasi yang diamati atau dicurigai melalui saluran yang sesuai pada waktu yang tepat.

A.7 Kontrol Fisik [14]

1.Perimeter keamanan fisik

Kontrol

Perimeter keamanan harus didefinisikan dan digunakan untuk memproteksi area yang berisi informasi dan aset terkait lainnya.

2.Entri fisik

Kontrol

Area aman harus diproteksi oleh kontrol entri dan titik akses yang tepat.

A.7.3 Mengamankan kantor, ruangan, dan fasilitas

Kontrol

Keamanan fisik untuk kantor, ruangan, dan fasilitas harus didesain dan diimplementasikan.

A.7 Kontrol Fisik [14]

4.Pemonitoran keamanan fisik

Kontrol

Premis harus terus dimonitor untuk menemukan akses fisik yang takterotorisasi.

5.Memproteksi dari ancaman fisik dan lingkungan

Kontrol

Proteksi terhadap ancaman fisik dan lingkungan, seperti bencana alam dan ancaman fisik yang disengaja atau tidak disengaja lainnya terhadap infrastruktur harus didesain dan diimplementasikan.

A.7.6 Bekerja di area yang aman

Kontrol

Langkah-langkah keamanan untuk bekerja di area aman harus didesain dan diimplementasikan.

A.7 Kontrol Fisik [14]

7.Meja bersih dan layar bersih

Kontrol

Aturan meja bersih untuk kertas dan media penyimpanan yang dapat dipindahkan serta aturan layar bersih untuk fasilitas pemrosesan informasi harus didefinisikan dan ditegakkan dengan tepat.

8.Penempatan dan proteksi peralatan

Kontrol

Peralatan harus ditempatkan dengan aman dan diproteksi.

9.Keamanan aset di luar lokasi

Kontrol

Aset di luar lokasi harus diproteksi.

A.7 Kontrol Fisik [14]

10.Media penyimpanan

Kontrol

Media penyimpanan harus dimanajemeni melalui siklus hidup akuisisi, penggunaan, transportasi, dan pembuangan sesuai dengan skema klasifikasi organisasi dan persyaratan penanganan.

11.Utilitas pendukung

Kontrol

Fasilitas pemrosesan informasi harus diproteksi dari kegagalan daya dan disrupsi lain yang disebabkan oleh kegagalan dalam utilitas pendukung.

12.Keamanan perkabelan

Kontrol

Kabel yang menyalurkan listrik, data, atau layanan informasi pendukung harus diproteksi dari intersepsi, interferensi, atau kerusakan.

A.7 Kontrol Fisik [14]

13.Pemeliharaan peralatan

Kontrol

Peralatan harus dipelihara dengan benar untuk memastikan availabilitas, integritas, dan konfidensialitas informasi.

14.Pemusnahan atau penggunaan kembali peralatan dengan aman

Kontrol

Peralatan yang berisi media penyimpanan harus diverifikasi untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dipindahkan atau ditimpa dengan aman sebelum dimusnahkan atau digunakan kembali.

A.8 Kontrol Teknologi [34]

1.Perangkat titik akhir pengguna

Kontrol

Informasi yang disimpan, diproses, atau dapat diakses melalu peranti titik akhir pengguna harus diproteksi.

2.Hak akses privilese

Kontrol

Alokasi dan penggunaan hak akses privilese harus dibatasi dan dimanajemeni.

3.Pembatasan akses informasi

Kontrol

Akses ke informasi dan aset terkait lainnya harus dibatasi sesuai dengan kebijakan topik spesifik yang ditetapkan pada kontrol akses.

A.8 Kontrol Teknologi [34]

4.Akses ke kode sumber

Kontrol

Akses untuk membaca dan menulis ke kode sumber, alat pengembangan, dan pustaka perangkat lunak harus dimanajemeni dengan tepat.

5.Autentikasi aman

Kontrol

Teknologi dan prosedur autentikasi yang aman harus diimplementasikan berdasarkan pembatasan akses informasi dan kebijakan topik spesifik pada kontrol akses.

6.Manajemen kapasitas

Kontrol

Penggunaan sumber daya harus dimonitor dan disesuaikan sejalan dengan persyaratan kapasitas saat ini dan yang diharapkan.

A.8 Kontrol Teknologi [34]

7.Proteksi terhadap perangkat perusak

Kontrol

Proteksi terhadap perangkat perusak harus diimplementasikan dan didukung oleh kesadaran pengguna yang tepat.

8.Manajemen kerentanan teknis

Kontrol

Informasi kerentanan teknis dari sistem informasi yang sedang digunakan harus diperoleh, eksposur organisasi terhadap kerentanan tersebut harus dievaluasi, dan langkah- langkah yang tepat harus diambil.

A.8 Kontrol Teknologi [34]

9.Manajemen konfigurasi

Kontrol

Konfigurasi, termasuk konfigurasi keamanan, perangkat keras, perangkat lunak, layanan, dan jaringan harus ditetapkan, didokumentasikan, diimplementasikan, dimonitor, dan direviu.

10.Penghapusan informasi

Kontrol

Informasi yang disimpan dalam sistem informasi, peranti atau di media penyimpanan lainnya harus dihapus bila tidak lagi diperlukan.

A.8 Kontrol Teknologi [34]

11.Penyamaran (masking) data

Kontrol

Penyamaran data harus digunakan sesuai dengan kebijakan topik spesifik organisasi tentang kontrol akses dan kebijakan topik spesifik terkait lainnya, serta persyaratan bisnis, konsiderasi legislasi yang berlaku.

12.Pencegahan kebocoran data

Kontrol

Langkah-langkah pencegahan kebocoran data harus diterapkan pada sistem, jaringan, dan peranti lain yang memproses, menyimpan, atau mentransmisikan informasi sensitif.

A.8 Kontrol Teknologi [34]

13.Pencadangan informasi

Kontrol

Salinan cadangan informasi, perangkat lunak, dan sistem harus dipelihara dan diuji secara reguler sesuai dengan kebijakan topik spesifik yang disepakati tentang pencadangan.

14.Redundansi fasilitas pemrosesan informasi

Kontrol

Fasilitas pemrosesan informasi harus diimplementasikan dengan redundansi yang cukup untuk memenuhi persyaratan availabilitas.

15.Membuat log

Kontrol

Log yang merekam aktivitas, eksepsi, kesalahan, dan peristiwa relevan lainnya harus diproduksi, disimpan, diproteksi, dan dianalisis.

A.8 Kontrol Teknologi [34]

16.Pemonitoran aktivitas

Kontrol

Jaringan, sistem, dan aplikasi harus dimonitor untuk menemukan perilaku anomali dan mengambil tindakan yang tepat untuk mengevaluasi potensi insiden keamanan informasi.

17.Sinkronisasi jam

Kontrol

Jam sistem pemrosesan informasi yang digunakan oleh organisasi harus disinkronkan ke sumber waktu yang disetujui.

18.Penggunaan program utilitas privilese

Kontrol

Penggunaan program utilitas yang mampu membatalkan sistem dan kontrol aplikasi harus dibatasi dan dikontrol dengan ketat.

A.8 Kontrol Teknologi [34]

19.Instalasi perangkat lunak pada sistem operasional

Kontrol

Prosedur dan langkah-langkah harus diimplementasikan untuk memanajemeni instalasi perangkat lunak dengan aman pada sistem operasional.

20.Keamanan jaringan

Kontrol

Jaringan dan peranti jaringan harus diamankan, dimanajemeni, dan dikontrolkan untuk memproteksi informasi dalam sistem dan aplikasi.

21.Keamanan layanan jaringan

Kontrol

Mekanisme keamanan, level layanan, dan persyaratan layanan jaringan harus diidentifikasi, diimplementasikan, dan dimonitor.

A.8 Kontrol Teknologi [34]

22.Segregasi jaringan

Kontrol

Kelompok layanan informasi, pengguna, dan sistem informasi harus dipisahkan dalam jaringan organisasi.

23.Pemfilteran web

Kontrol

Akses ke situs web eksternal harus dimanajemeni untuk mengurangi eksposur konten berbahaya.

24.Penggunaan kriptografi

Kontrol

Aturan untuk penggunaan kriptografi yang efektif, termasuk manajemen kunci kriptografi, harus didefinisikan dan diimplementasikan.

A.8 Kontrol Teknologi [34]

A.8.25 Siklus hidup pengembangan yang aman

Kontrol

Aturan untuk pengembangan perangkat lunak dan sistem yang aman harus ditetapkan dan diterapkan.

26.Persyaratan keamanan aplikasi

Kontrol

Persyaratan keamanan informasi harus diidentifikasi, dispesifikasi, dan disetujui saat mengembangkan atau memperoleh aplikasi.

27.Prinsip-prinsip arsitektur dan rekayasa sistem yang aman

Kontrol

Prinsip-prinsip untuk rekayasa sistem yang aman harus ditetapkan, didokumentasikan, dipelihara, dan diterapkan pada segala aktivitas pengembangan sistem informasi.

A.8 Kontrol Teknologi [34]

28.Pengkodean yang aman

Kontrol

Prinsip pengkodean yang aman harus diterapkan pada pengembangan perangkat lunak.

29.Pengujian keamanan dalam pengembangan dan penerimaan

Kontrol

Proses pengujian keamanan harus didefinisikan dan diimplementasikan dalam siklus hidup pengembangan.

30.Pengembangan yang dialihdayakan

Kontrol

Organisasi harus mengarahkan, memonitor, dan mereviu aktivitas yang terkait dengan pengembangan sistem yang dialihdayakan.

A.8 Kontrol Teknologi [34]

31.Pemisahan lingkungan pengembangan, pengujian, dan produksi

Kontrol

Lingkungan pengembangan, pengujian, dan produksi harus dipisahkan dan diamankan.

32.Manajemen perubahan

Kontrol

Perubahan fasilitas pemrosesan informasi dan sistem informasi harus menjadi subyek bagi prosedur manajemen perubahan.

A.8 Kontrol Teknologi [34]

33.Informasi uji

Kontrol

Informasi uji harus dipilih, diproteksi, dan dimanajemeni secara tepat.

34.Proteksi sistem informasi selama pengujian audit

Kontrol

Uji audit dan aktivitas keyakinan lainnya yang melibatkan asesmen sistem operasional harus direncanakan dan disepakati antara penguji dan manajemen yang tepat.

Untuk memudahkan implementasi kontrol SMKI, dapat merujuk kepada SNI ISO/IEC 27002:2022

Tugas Klausul 8

1. Peserta membuat flowchart bisnis proses: (pililh 2)

a. Pengelolaan akses

b. Pengelolaan email

c. Pengelolaan asset TIK

d. Pengelolaan SDM

e. Teleworking

TERIMA KASIH