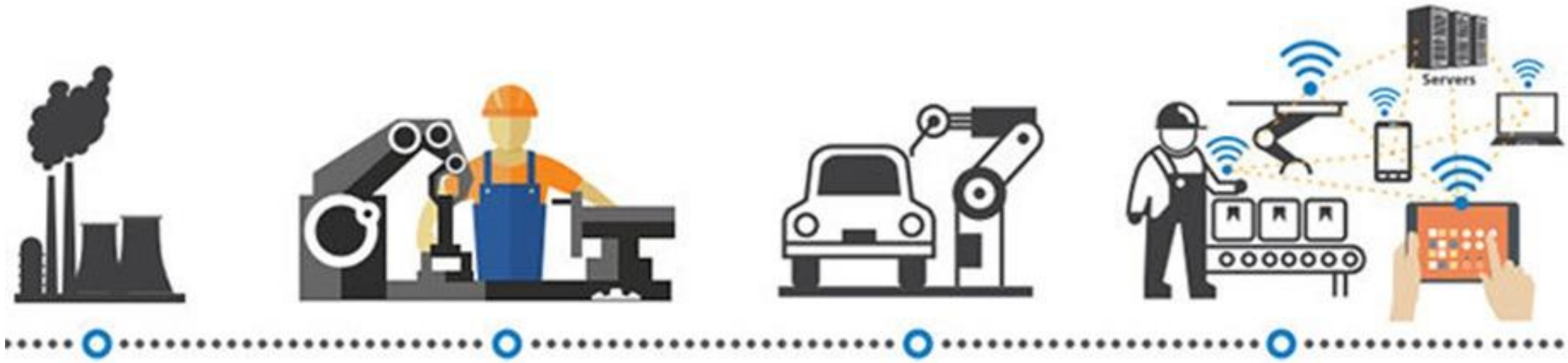
SISTEM MANAJEMEN PENGAMANAN INFORMASI (SMPI)

PILAR
TEKNOTAMA SINERGI

...Persistent to Innovate by Technology & Shared Information...

LATAR BELAKANG

Perkembangan industri



Tren teknologi

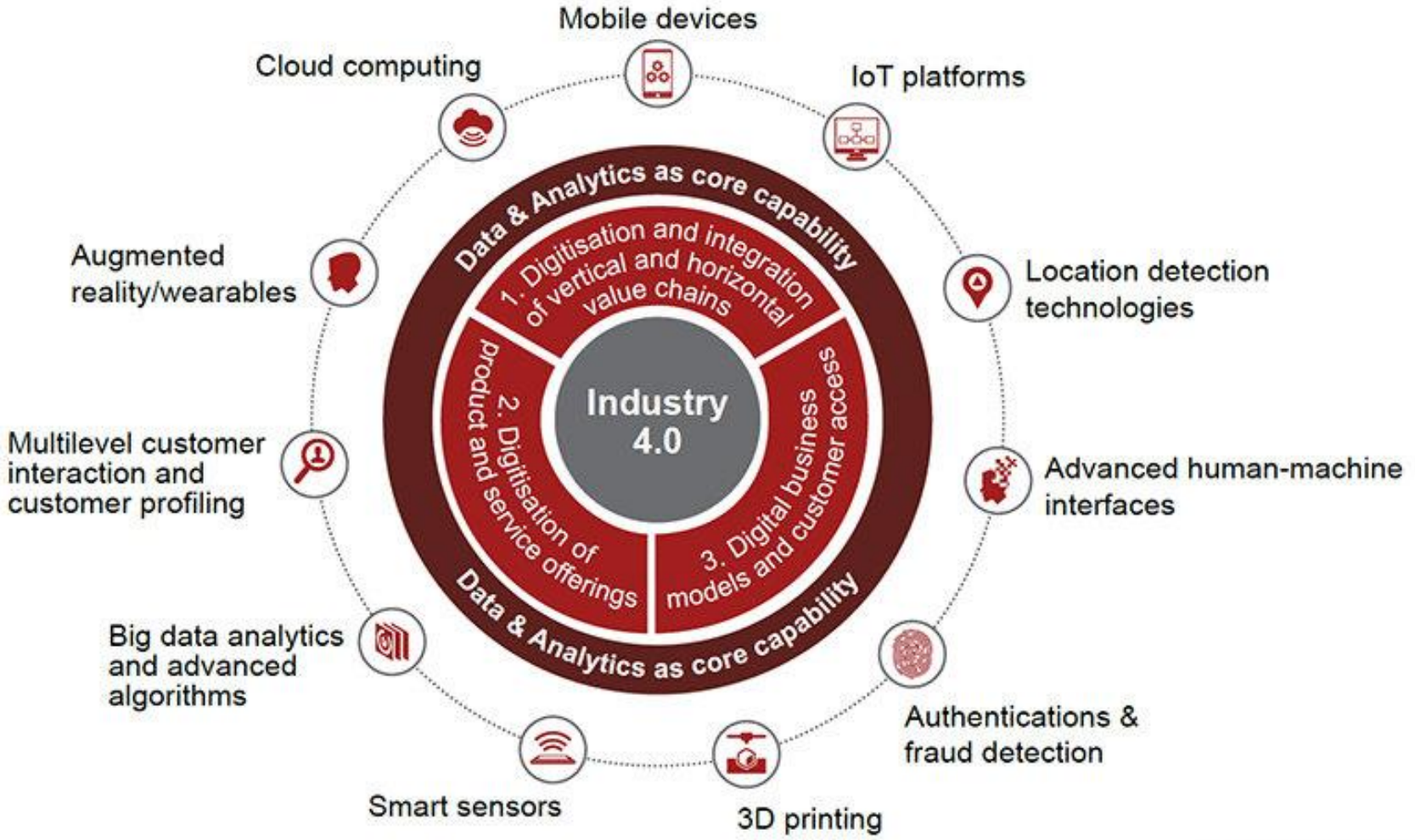
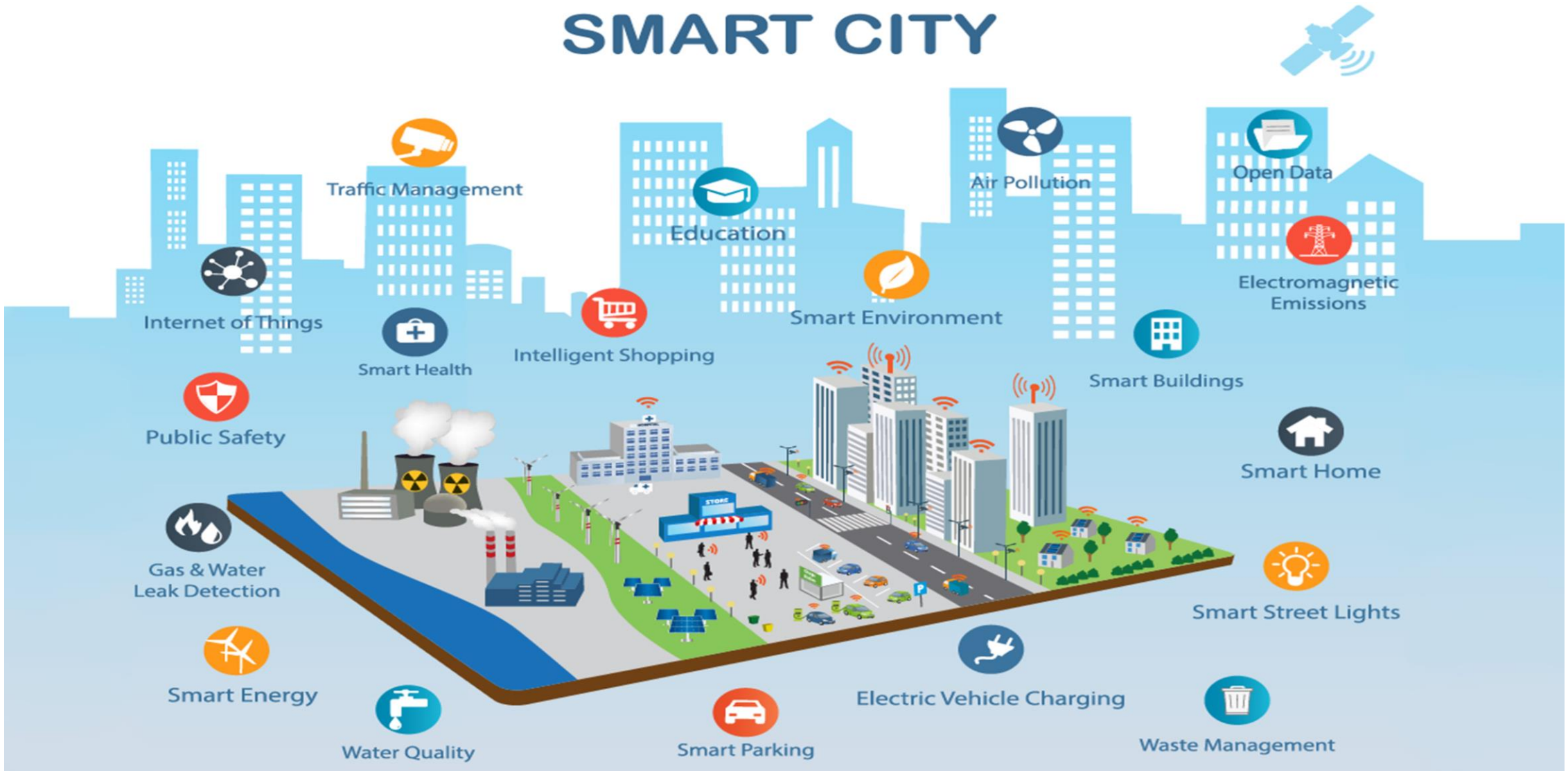
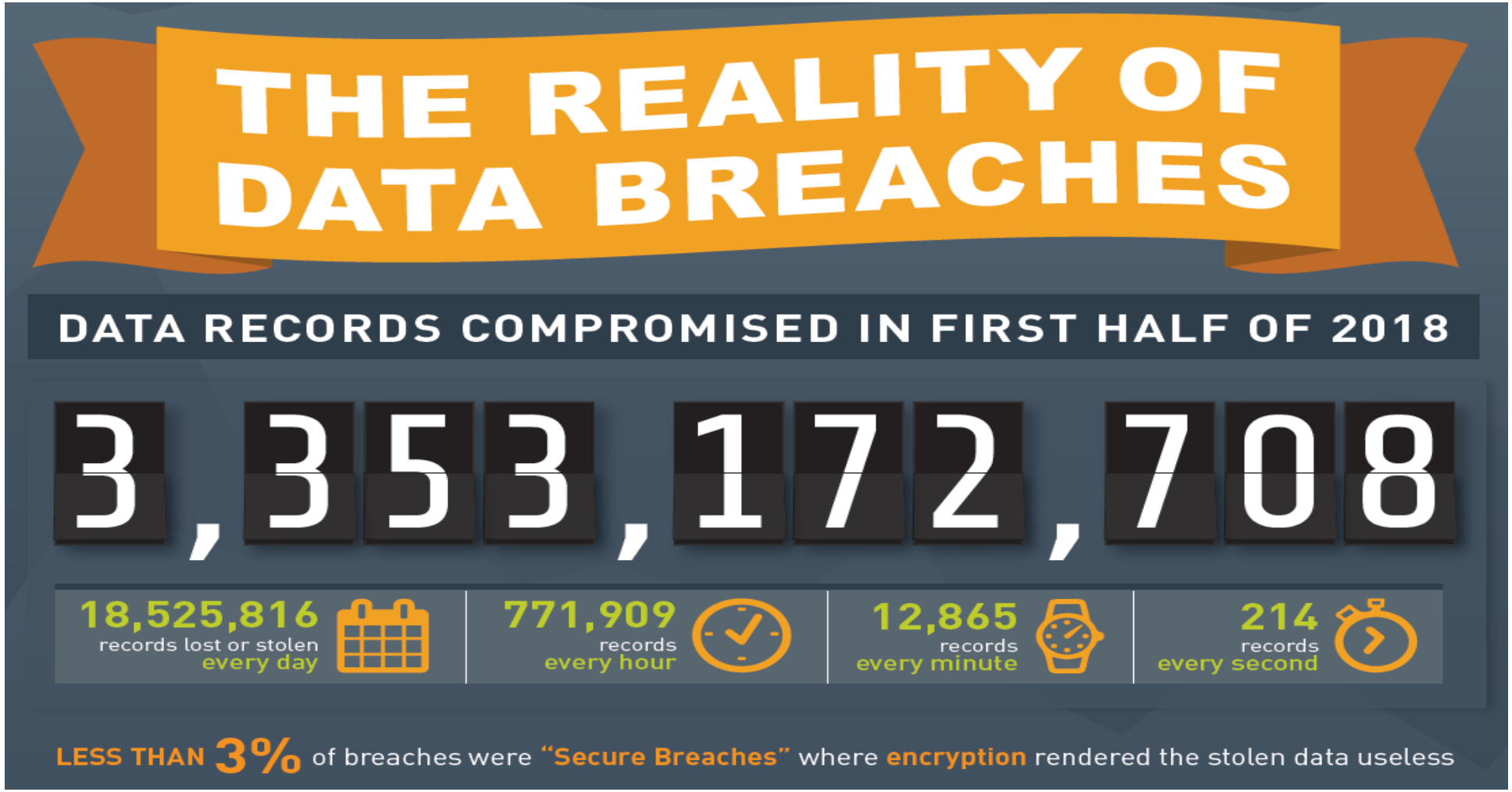


image source: PwC

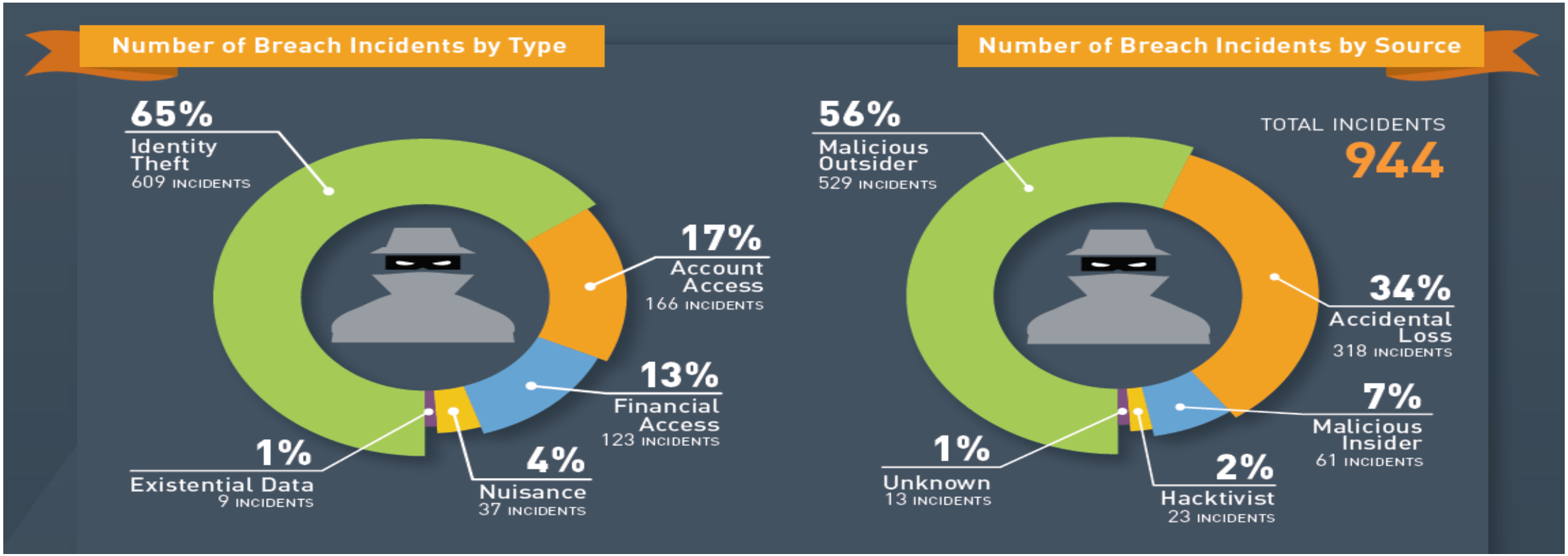

SMART CITY
Traffic Management
Education
Air Pollution
Open Data
Internet of Things
Smart Health
Intelligent Shopping
Smart Environment
Electromagnetic Emissions
Smart Buildings
Public Safety
Smart Home
Gas & Water Leak Detection
Smart Street Lights
Smart Energy
Electric Vehicle Charging
Water Quality
Smart Parking
Waste Management

Infografis Insiden Keamanan Informasi Dunia



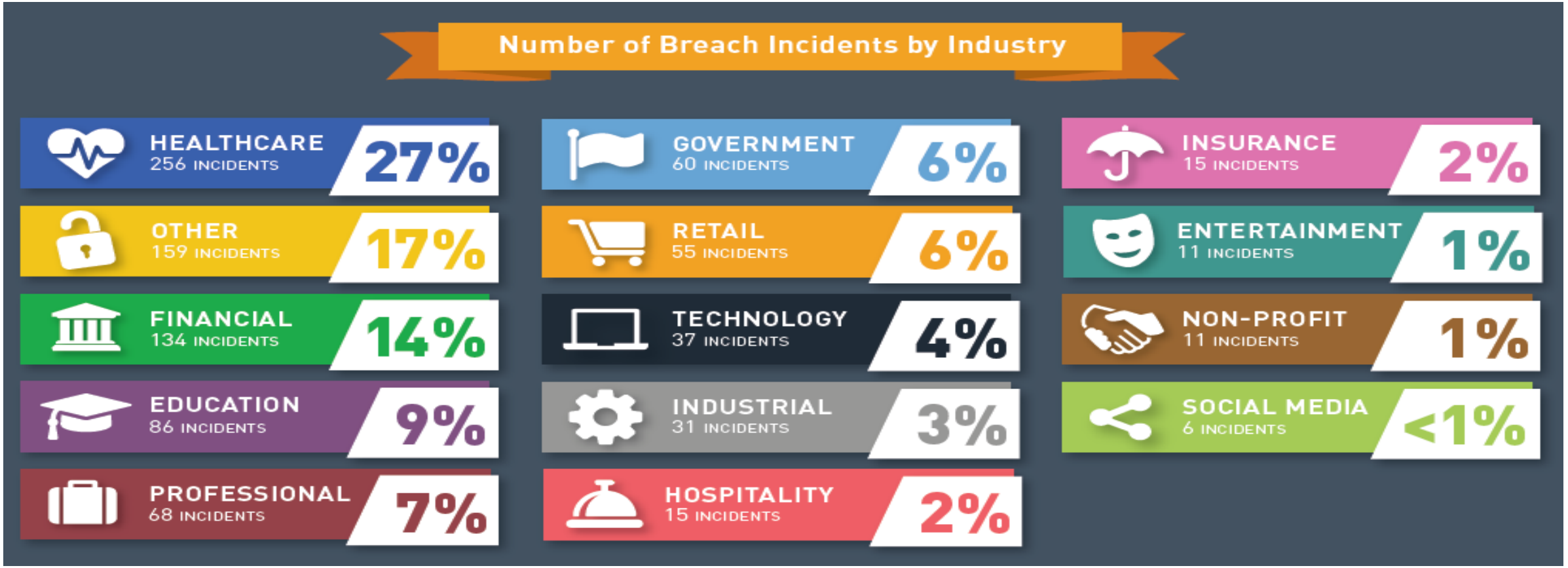
https://breachlevelindex.com

Infografis Insiden Keamanan Informasi Dunia



https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Infografis Insiden Keamanan Informasi Dunia



- Data statistik kehilangan informasi dunia:

Top Scoring Data Breaches

By Risk Score | By Industry | By Type | By Source

Organization Breached	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location	Industry	Risk Score
Facebook	2,200,000,000	04/04/18	Identity Theft	Malicious Outsider	United States	Social Media	10.0
Equifax	147,900,000	07/15/17	Identity Theft	Malicious Outsider	United States	Financial	10.0
Reliance Jio	120,000,000	07/10/17	Account Access	Malicious Outsider	India	Technology	10.0
Friend Finder Networks	412,214,295	10/16/16	Existential Data	Malicious Outsider	United States	Entertainment	10.0
Anthem Insurance Companies (Anthem Blue Cross)	78,800,000	01/27/15	Identity Theft	State Sponsored	United States	Healthcare	10.0
Yahoo	500,000,000	12/01/14	Account Access	State Sponsored	United States	Technology	10.0
Home Depot	109,000,000	09/02/14	Financial Access	Malicious Outsider	United States	Retail	10.0
JPMorgan Chase	83,000,000	08/27/14	Identity Theft	Malicious Outsider	United States	Financial	10.0
CyberVor	1,200,000,000	08/05/14	Account Access	Malicious Outsider	Global	Technology	10.0
eBay	145,000,000	05/21/14	Identity Theft	Malicious Outsider	United States	Retail	10.0
Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card	104,000,000	01/20/14	Identity Theft	Malicious Insider	South Korea	Financial	10.0
Target	110,000,000	11/04/13	Financial Access	Malicious Outsider	United States	Retail	10.0
Adobe Systems, Inc	152,000,000	09/18/13	Financial Access	Malicious Outsider	United States	Technology	10.0
Yahoo	1,000,000,000	08/09/13	Identity Theft	Malicious Outsider	United States	Technology	10.0
MySpace	360,000,000	06/11/13	Account Access	Malicious Outsider	United States	Other	10.0
Motor Vehicles Department in Kerala	200,000,000	05/01/17	Nuisance	Malicious Outsider	India	Government	9.9
General Directorate of Population and Citizenship Affairs, the General Directorate of Land Registry and Cadaster	50,000,000	01/12/15	Identity Theft	Malicious Outsider	Turkey	Government	9.9
Country's Supreme Election Committee (YSK)	54,000,000	12/16/13	Identity Theft	Malicious Outsider	Turkey	Government	9.9
iMesh	51,000,000	09/22/13	Identity Theft	Malicious Outsider	United States	Technology	9.9
River City Media	1,340,000,000	03/06/17	Nuisance	Accidental Loss	United States	Other	9.8

Infografis insiden keamanan informasi di Indonesia

KEJADIAN DI SEKTOR PEMERINTAH

Serangan terjadi dalam bentuk *Distributed Denial of Service* terhadap *web service* milik pemerintah, bank, media, dan partai politik. Puluhan ribu pengunjung serentak mengakses *web service* tersebut yang menyebabkan lumpuhnya system.

2007 - Estonia mengalami serangan siber yang mengakibatkan kegagalan di banyak sektor terutama pemerintahan, transportasi, energi, dan keuangan.

Ditengarai, serangan berasal dari Rusia sebagai aksi atas relokasi monumen memorial era perang Soviet di Tallinn, yang menyebabkan ketegangan hubungan diplomatik kedua negara

- Kekuatan diplomasi, untuk mengangkat isu ini dalam parlemen Uni Eropa dan pertemuan NATO
- Dibangunnya NATO Cooperative Cyber Defense Center of Excellence di Estonia

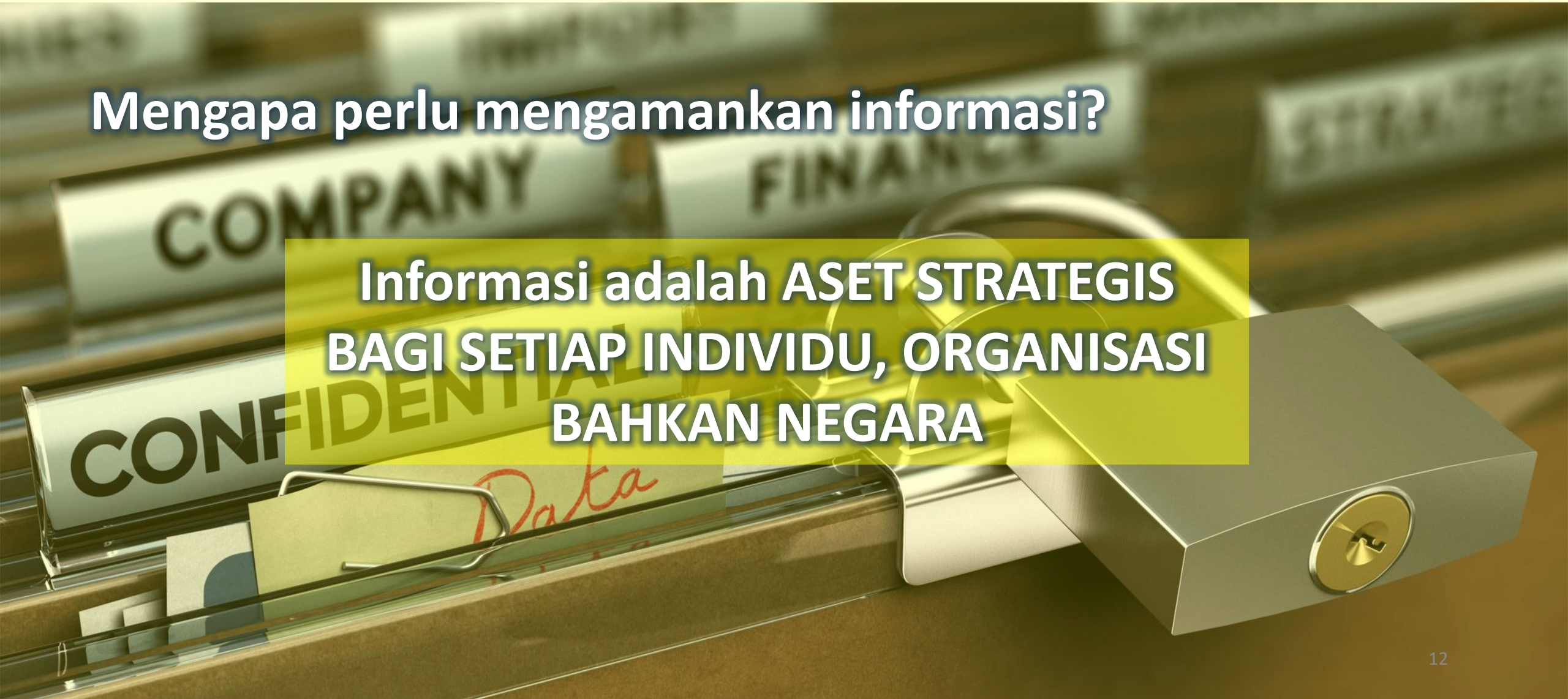
Sumber:
Dirangkum dari berbagai sumber

SERANGAN TERHADAP INFRASTRUKTUR VITAL

AND…

WHO's NEXT?

TUJUAN



Mengapa perlu mengamankan informasi?

Informasi adalah ASET STRATEGIS BAGI SETIAP INDIVIDU, ORGANISASI BAHKAN NEGARA

PRINSIP DAN KONSEP

Cara Pandang

Tradisional

- Masih menjadi domain dari *System Administrator*
- Lebih banyak dengan pengadaan *Firewall*
- Implementasi pengendalian keamanan bukanlah sebuah keharusan

PRINSIP DAN KONSEP

Cara Pandang

Modern

- Menjadi pokok perhatian pemilik bisnis
- Aktifitas mencari tahu risiko dan pada saat yang sama menemukan solusi yang tepat
- Bisnis dan keamanan menjadi bagian yang tidak dapat dipisahkan
- Tim keamanan terdiri dari *Top Management, IT Managers and a Dedicated Information Security Manager*
- Penggunaan model *Plan, Do, Check and Act*
- Integrasi ke sistem kualitas dengan menggunakan standar ISO, CMMI, dll dengan memusatkan pada model keamanan informasi

PRINSIP DAN KONSEP

CIA Triad

PRINSIP DAN KONSEP

Tujuan Pengamanan Informasi:

- ***Confidentiality* (Kerahasiaan)**
  - ✓ Memberikan informasi yang dapat dipercaya dari pemilik informasi yang sah kepada pihak yang berhak menerima informasi tersebut
- ***Integrity* (Keutuhan)**
  - ✓ Menjaga dan melindungi informasi dari kehilangan keutuhan dan atau modifikasi yang tidak sesuai dengan keutuhan informasi dari sejak informasi itu diterima, diolah, disimpan, dan ditranfer/ditransmisikan
- ***Availability* (Ketersediaan)**
  - ✓ Informasi yang diberikan kepada pihak yang berhak menerimanya dapat tersedia ketika dibutuhkan dan ada sepanjang waktu

REGULASI DAN KERANGKA KERJA

Regulasi Nasional

SEKTOR	KEBIJAKAN	ATURAN TEKNIS
Publik	Information and Electronic Transaction / Undang-Undang Informasi dan Transaksi Elektronik(UU No.11 2008)	-
Pemerintahan	Peraturan Presiden Nomor 95 Tahun 2018 Mengenai Sistem Pemerintahan Berbasis Elektronik (SPBE)	Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi (SMPI)
Perbankan	Peraturan Otoritas Jasa Keuangan Nomor 38 /POJK.03/2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum	Surat Edaran Otoritas Jasa Keuangan Nomor 34 /SEOJK.03/2016 Tentang Penerapan Manajemen Risiko Bagi Bank Umum
BUMN	Peraturan Menteri BUMN PER-02/MBU/02/2018 Tentang Prinsip Tata Kelola Teknologi Informasi Kementerian Badan Usaha Milik Negara	-

REGULASI DAN KERANGKA KERJA

Regulasi Internasional

SEKTOR	KEBIJAKAN	SUMBER
Pemerintahan	Regulation (EU) 2016/679 (EU General Data Protection Regulation (EU GDPR))	Uni Eropa
Perbankan	Basel II: BASEL capital accord (April 2003) (Basel Committee on Banking Supervision)	Global
Publik	Federal Information Security Management Act of 2002 (FISMA)	USA
Perdagangan	Free and Secure Trade Program (FAST)	USA

REGULASI DAN KERANGKA KERJA

Kerangka Kerja (*framework*)

INSTITUSI	STANDAR
ISACA	COBIT 5 (Control Objectives for Information and Related Technologies)
International Organization for Standardization	ISO/IEC 27000 family - Information Security Management Systems
PCI Security Standards Council	PCI Data Security Standard (PCI DSS)
AXELOS	Information Technology Infrastructure Library (ITIL)
The Open Group	The Open Group Architecture Framework (TOGAF)
NIST	Special Publication 800-100: Information Security Handbook

STANDAR MANAJEMEN PENGAMANAN INFORMASI (SMPI) BERBASIS ISO 27001

BAB IV

PENYELENGGARAAN

Bagian Kesatu

Penyelenggara Sistem Elektronik

Pasal 10

(1) Penyelenggara Sistem Elektronik strategis dan Penyelenggara Sistem Elektronik tinggi wajib memiliki Sertifikat Sistem Manajemen Pengamanan Informasi.

(2) Penyelenggara Sistem Elektronik rendah dapat memiliki Sertifikat Sistem Manajemen Pengamanan Informasi.

ISO 27001

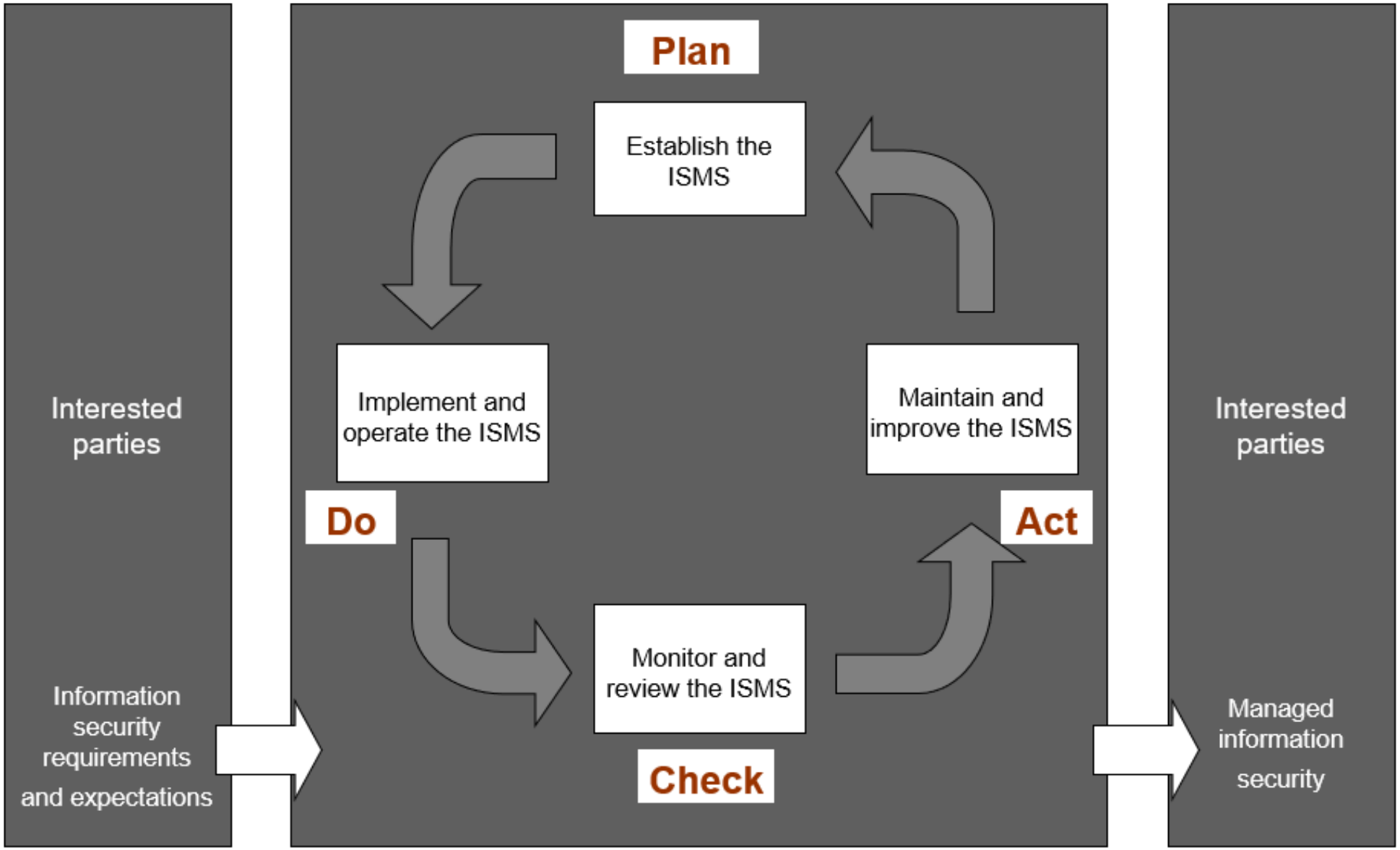
- **ISO 27001:2013** adalah standar untuk keamanan informasi
- Merupakan spesifikasi untuk Sistem Manajemen Pengamanan Informasi (SMPI)
- Dirancang untuk melindungi beragam* informasi yang dibutuhkan

**scope didefinisikan oleh organisasi*

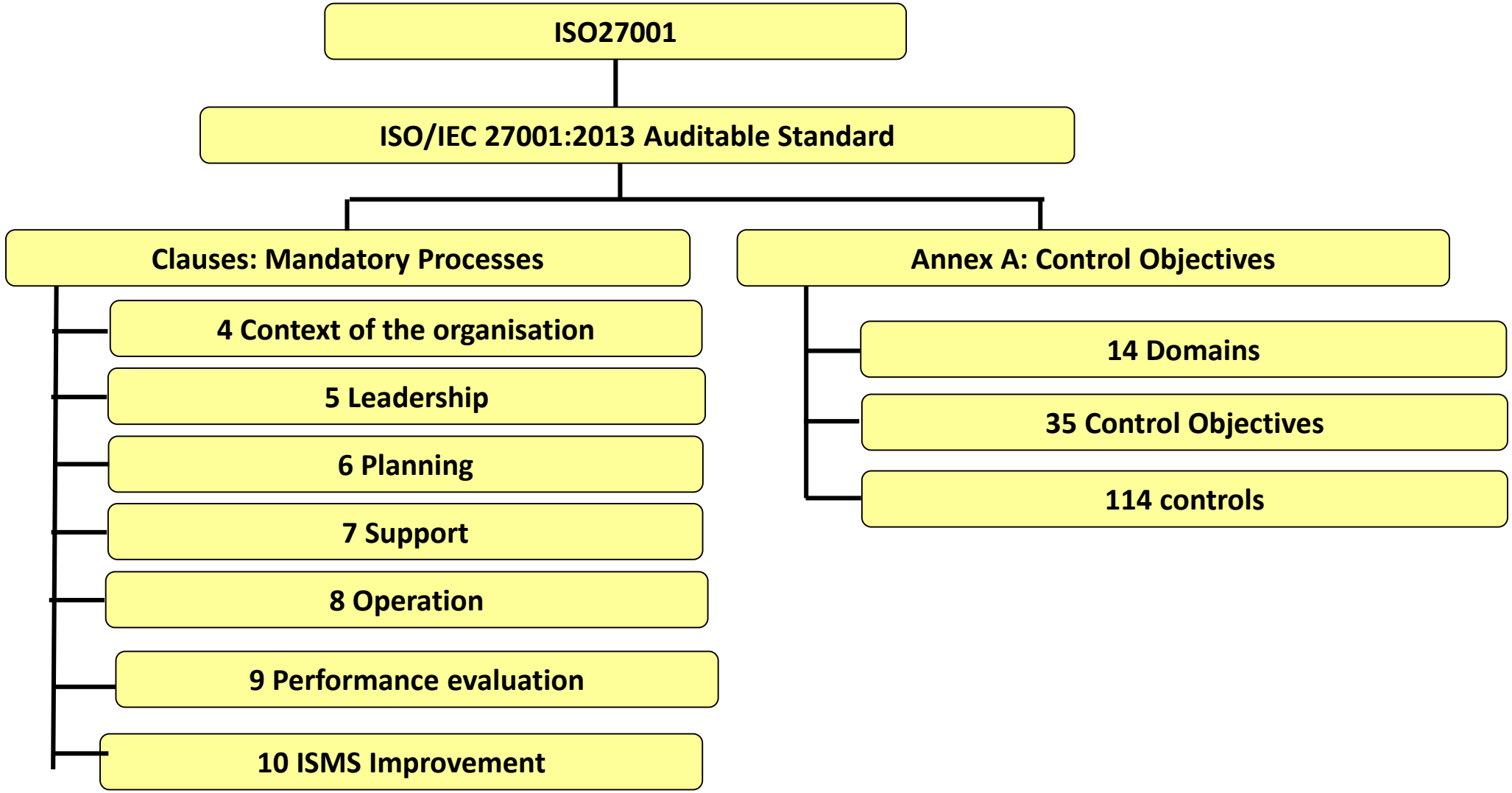
ISO 27001

- Adopsi SMPI adalah keputusan strategis.
- Rancangan dan implementasi SMPI dipengaruhi oleh tujuan bisnis dan tujuan keamanan, kebutuhan risiko dan pengendalian keamanan, proses yang dijalankan serta ukuran dan struktur organisasi.
  - Sebuah organisasi yang sederhana membutuhkan SMPI yang sederhana.
- SMPI akan berkembang secara sistematis sebagai respon atas berubahnya risiko.
- Kepatuhan dengan ISO27001 dapat dinilai dan disertifikasi.

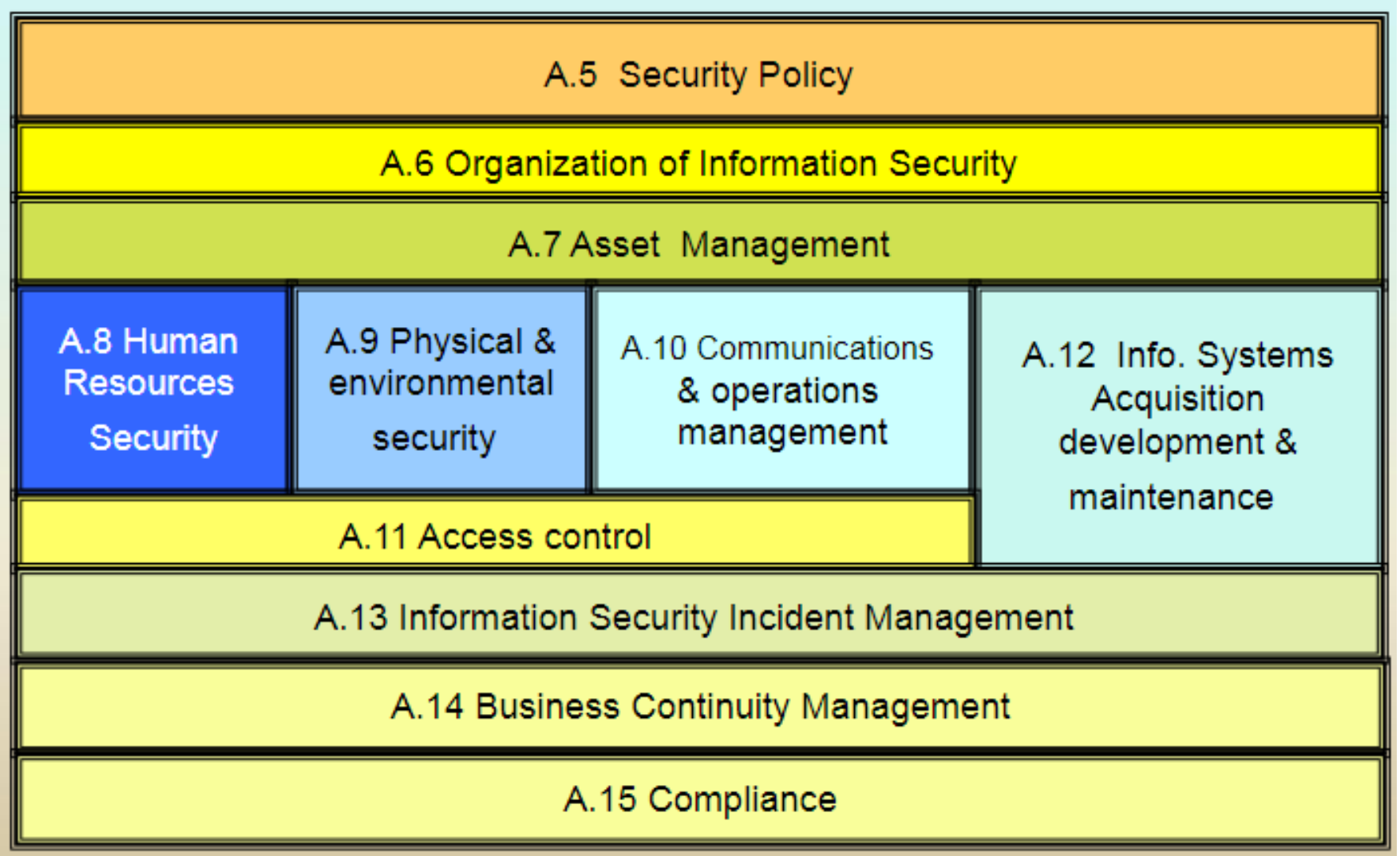
ISO 27001


Interested parties
Information security requirements and expectations
Plan
Establish the ISMS
Do
Implement and operate the ISMS
Check
Monitor and review the ISMS
Act
Maintain and improve the ISMS
Interested parties
Managed information security

Struktur ISO 27001



Struktur Kontrol (Annex A)



Persyaratan Utama Implementasi

Persyaratan utama yang harus dipenuhi menyangkut:

- Sistem manajemen pengamanan informasi (kerangka kerja, proses dan dokumentasi)
- Tanggung jawab manajemen
- Audit internal SMPI
- Manajemen tinjau ulang (*management review*) SMPI
- Peningkatan berkelanjutan

Dokumentasi SMPI

- Struktur Dokumentasi SMPI

Dokumentasi SMPI

- Dokumen Tingkat 1
  - Merupakan dokumen dengan hirarki tertinggi dalam struktur dokumentasi SMPI.
  - Dokumen ini bersifat strategis yang memuat komitmen yang dituangkan dalam bentuk kebijakan, standar, sasaran dan rencana terkait pengembangan (*development*), penerapan (*implementation*) dan peningkatan (*improvement*) sistem manajemen keamanan informasi.
  - Dokumen Tingkat 1 minimum terdiri dari:
    a. Kebijakan Keamanan Informasi
    b. Peran dan tanggung jawab organisasi keamanan informasi
    c. Klasifikasi informasi
    d. Kebijakan Pengamanan Akses Fisik dan Lojik
    e. Kebijakan Manajemen Risiko TIK
    f. Manajemen Kelangsungan Usaha (*Business Continuity Management*)
    g. Ketentuan Penggunaan Sumber Daya TIK

Dokumentasi SMPI

- Dokumen Tingkat 2
  - Dokumen tingkat 2 ini umumnya meliputi prosedur dan panduan yang dikembangkan secara internal oleh instansi/lembaga penyelenggara pelayanan publik dan memuat cara menerapkan kebijakan yang telah ditetapkan serta menjelaskan penanggung jawab kegiatan.
  - Dokumen ini bersifat operasional.
  - Prosedur-prosedur dalam dokumen tingkat 2 meliputi antara lain:
    a. Prosedur pengendalian dokumen
    b. Prosedur pengendalian rekaman
    c. Prosedur audit internal SMPI
    d. Prosedur tindakan perbaikan dan pencegahan
    e. Prosedur penanganan informasi (penyimpanan, pelabelan, pengiriman/pertukaran, pemusnahan)
    f. Prosedur penanganan insiden/gangguan keamanan informasi
    g. Prosedur pemantauan penggunaan fasilitas teknologi informasi

Dokumentasi SMPI

- Dokumen Tingkat 3
  - Dokumen tingkat 3 meliputi petunjuk teknis, instruksi kerja dan formulir yang digunakan untuk mendukung pelaksanaan prosedur tertentu sampai ke tingkatan teknis. Instruksi kerja tidak selalu diperlukan untuk setiap prosedur. Sepanjang prosedur sudah menguraikan langkah-langkah aktivitas yang jelas dan mudah dipahami penanggung jawab kegiatan, petunjuk teknis / instruksi kerja tidak diperlukan lagi.

Tahapan Penerapan SMPI

Tahapan Penerapan SMPI

1. Persetujuan Pimpinan

- Setiap proyek memerlukan investasi baik untuk penyediaan sumber daya maupun untuk pelatihan yang diperlukan. Pimpinan harus memberikan persetujuannya terhadap rencana investasi tersebut.
- Sebelum rencana penerapan SMPI, pimpinan harus mendapatkan penjelasan yang memadai tentang seluk beluk, nilai penting dan untung rugi menerapkan SMPI serta konsekuensi ataupun komitmen yang dibutuhkan dari pimpinan sebagai tindak lanjut persetujuan terhadap proyek SMPI.

Tahapan Penerapan SMPI

1. Persetujuan Pimpinan

- Persetujuan pimpinan harus diikuti dengan arahan dan dukungan selama berlangsungnya proyek tersebut. Oleh karena itu, perkembangan proyek SMPI harus dikomunikasikan secara berkala kepada pimpinan pasca persetujuannya agar setiap masalah yang memerlukan pengambilan keputusan pimpinan dapat diselesaikan secara cepat dan tepat.

Tahapan Penerapan SMPI

2. Menetapkan Organisasi, Peran dan Tanggungjawab

- Organisasi atau tim SMPI harus ditetapkan secara formal dan diketuai oleh koordinator atau ketua tim.
- Jumlah anggota tim disesuaikan dengan ruang lingkup organisasinya.
- Tugas utama tim ini adalah menyiapkan, menjamin dan/atau melakukan seluruh kegiatan dalam tahapan penerapan SMPI agar dapat terlaksana dengan baik sesuai rencana.

Tahapan Penerapan SMPI

2. Menetapkan Organisasi, Peran dan Tanggungjawab

- Organisasi penanggung jawab keamanan informasi ini dapat ditetapkan sebagai struktur organisasi yang bersifat permanen atau sebagai “tim adhoc” (tim proyek) sesuai kebutuhan.
- Tanggungjawab ketua dan anggota tim serta unit kerja terkait dalam hal keamanan informasi harus diuraikan secara jelas.
- Ketua tim hendaknya ditetapkan/dipilih dari pejabat tertinggi sesuai ruang lingkup penerapan SMPI atau yang pejabat yang didelegasikan.

Tahapan Penerapan SMPI

3. Mendefinisikan Ruang Lingkup

- Ruang lingkup ini meliputi:
  - Proses dan/atau Kegiatan. Misalnya: Penyediaan layanan publik, Pengamanan Pusat Data, pengembangan aplikasi, penggunaan jaringan dan fasilitas email, dan sebagainya.
  - Satuan Kerja. Misalnya: Direktorat, Departemen atau Bidang.
  - Lokasi kerja. Misalnya: Tingkat Pusat, daerah atau keduanya. Mana saja lokasi yang dipilih untuk menerapkan SMPI? Apakah SMPI akan langsung diterapkan ke seluruh lokasi kerja? Atau apakah diterapkan secara bertahap dengan memprioritaskan pada lokasi tertentu terlebih dahulu?

Tahapan Penerapan SMPI

3. Mendefinisikan Ruang Lingkup

- Penetapan ruang lingkup ini harus didiskusikan dengan Satuan Kerja terkait dengan memperhatikan tingkat kesiapan masing-masing termasuk ketersediaan sumber daya yang diperlukan untuk membangun dan menerapkan SMPI.

Tahapan Penerapan SMPI

4. Melakukan Gap Analysis

- Kegiatan ini dilakukan dengan tujuan utamanya untuk membandingkan seberapa jauh persyaratan klausul-klausul ISO 27001 telah dipenuhi, baik pada aspek kerangka kerja (kebijakan dan prosedur) maupun aspek penerapannya.
- Untuk aspek kerangka kerja, identifikasilah apakah kebijakan dan prosedur telah dipenuhi. Sedang untuk aspek penerapan, periksalah ketersediaan rekaman sebagai bukti-bukti penerapan.
- *Gap Analysis* umumnya dilakukan dengan bantuan *checklist* pemeriksaan. Selain *Checklist* Indeks KAMI, c*hecklist* lain untuk kegiatan *gap analysis* ISO 27001 dapat diunduh dari berbagai situs tentang keamanan informasi.

Tahapan Penerapan SMPI

6. Menetapkan Kontrol dan Sasaran Kontrol

- Dari hasil identifikasi risiko kemudian dipilih kontrol dan sasaran kontrol ISO 27001 yang dapat diterapkan sesuai dengan ruang lingkup yang ditetapkan.
- Sasaran kontrol dapat ditetapkan sebagai sasaran keamanan informasi tahunan yang digunakan sebagai patokan untuk mengukur efektivitas penerapan SMPI pada periode yang ditetapkan.
- Sasaran keamanan informasi tahunan dapat ditetapkan sesuai hasil kajian risiko dan prioritas pembenahan dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.

Contoh Sasaran Kontrol

No	Kontrol ISO 27001	Sasaran
1	A.13.1 Pengelolaan insiden	Menurunkan jumlah insiden karena virus sebanyak 10% dibanding tahun sebelumnya.
2	A.8.3.3 Penutupan hak akses	Hak akses user yang menjalani mutasi/ berhenti bekerja harus ditutup maksimum 2 hari setelah statusnya dilaporkan secara resmi.
3	A.9.1.2 Akses Data Center (Ruang Server)	Seluruh pihak ketiga (vendor, konsultan) yang memasuki Pusat Data harus didampingi karyawan
4	A.11.2.Manajemen password	80% perangkat komputer yang sensitif sudah menerapkan strong password

Tahapan Penerapan SMPI

7. Menetapkan Kebijakan dan Prosedur SMKI

- Kebijakan dan prosedur disusun dengan memperhatikan kontrol yang memang berlaku dan diterapkan dalam penyelenggaraan pelayanan publik.

Tahapan Penerapan SMPI

8. Sosialisasi dan Pelatihan

- Sosialisasi dapat dilakukan dengan berbagai cara, seperti:
  - Tatap muka di dalam kelas
  - Simulasi langsung di lokasi kerja
  - Penyampaian brosur, leaflet, spanduk untuk meningkatkan kepedulian karyawan
  - Penggunaan email, nota dinas, portal atau majalah internal
  - Media komunikasi lainnya

Tahapan Penerapan SMPI

8. Sosialisasi dan Pelatihan

- Untuk meningkatkan kompetensi personel, perlu dilakukan pelatihan yang lebih mendalam baik pada aspek teknis maupun tata kelola TIK.
- Berbagai jenis pelatihan menyangkut pengamanan informasi yang dapat diprogramkan, misalnya: **pengenalan ISO 27001, audit internal, pelatihan *lead auditor*, *risk management*, pelatihan untuk administrator** ataupun **jenis-jenis pelatihan untuk programmer.**
- Bukti sosialisasi dan pelatihan baik berupa materi, daftar hadir, hasil *pre/post test*, laporan evaluasi pelatihan ataupun sertifikat harus disimpan dan dipelihara.

Tahapan Penerapan SMPI

9. Menerapkan Kebijakan dan Prosedur

- Strategi penerapan/implementasi SMPI sebaiknya dilakukan dengan menyelaraskan kegiatan yang sedang berlangsung di instansi/lembaga.
- Hasil penerapan SMPI harus dicatat dalam bentuk laporan, log, rekaman atau isian formulir yang relevan yang mendukung kebijakan atau prosedur yang ditetapkan seperti laporan pencatatan insiden dan penyelesaiannya, daftar pengguna aplikasi, log aktivitas user, laporan pelatihan/sosialisasi, permintaan perubahan dan realisasinya, hasil pengujian aplikasi, laporan perawatan komputer, dan sebagainya.

Tahapan Penerapan SMPI

10. Mengukur Efektivitas Kontrol

- Kontrol yang telah ditetapkan baik berupa kebijakan, prosedur atau standar yang telah ditetapkan diukur efektivitasnya dengan mempelajari hasil-hasil penerapan yang dicatat atau dituliskan dalam laporan atau formulir-formulir yang relevan.
- Metode pengukuran kontrol harus ditetapkan terlebih dahulu, baru kemudian diukur efektivitas kontrolnya secara periodik sesuai kebutuhan dan karakteristik kegiatan.

Tahapan Penerapan SMPI

Contoh Pengukuran

Ketercapaian Sasaran SMPI

No	Kontrol ISO 27001	Sasaran	Metode Pengukuran	Frekuensi Pengukuran	Hasil Pengukuran
1	A.13.1 Pengelolaan insiden	Menurunkan jumlah insiden karena virus sebanyak 10% dibanding tahun sebelumnya.	Prosentase Jumlah insiden tajun lalu **dikurangi** prosentase Jumlah insiden sekarang	Per 3 bulan	
2	A.8.3.3 Penutupan hak akses	Seluruh hak akses user yang menjalani mutasi/ berhenti bekerja harus ditutup maksimum 2 hari setelah statusnya dilaporkan secara resmi.	Prosentase jumlah user yang telah ditutup hak aksesnya **dibagi** jumlah user mutasi atau keluar.	Per 6 bulan	
3	A.9.1.2 Akses Data Center (Ruang Server)	Seluruh (100%) pihak ketiga (vendor, konsultan) yang memasuki Pusat Data harus didampingi karyawan	Prosentase jumlah pihak ketiga yang memasuki Pusat Data dengan didampingi karyawan	Per 6 bulan	
4	A.11.2.3 Manajemen *password*	80% perangkat komputer yang sensitif sudah menerapkan *strong password*	Jumla PC dengan *strong password***diba gi** jumlah total PC	Per 6 bulan	

Tahapan Penerapan SMPI

11. Melakukan Audit Internal

- Audit internal dilakukan untuk menjamin agar penerapan SMPI dilakukan secara tepat sesuai dengan kebijakan dan prosedur yang ditetapkan.
- Audit internal harus dilakukan oleh personel/tim yang memiliki kompetensi di bidang audit TIK dan tidak melaksanakan kegiatan yang diaudit. Personel/tim yang melakukan audit internal harus ditetapkan oleh pimpinan/pejabat yang berwenang melalui Surat Keputusan atau Surat Penugasan yang resmi.
- Audit internal dapat dilakukan oleh pihak eksternal yang diminta secara resmi oleh instansi penyelenggara pelayanan publik.

Tahapan Penerapan SMPI

12. Melakukan Evaluasi,Peninjauan (Review) dan Penyempurnaan

- Implementasi seluruh kebijakan, prosedur atau standar yang ditetapkan kemudian dievaluasi efektivitasnya.
- Hasil pengukuran efektivitas kontrol dan laporan audit internal juga dievaluasi untuk diperiksa mana kontrol yang belum mencapai sasaran, masih lemah (belum efektif) atau yang masih menjadi temuan dalam audit internal.
- Seluruh kelemahan kontrol harus segera diperbaiki ataupun disempurnakan sehingga tidak menimbulkan kelemahan/kesalahan yang sama di kemudian hari.

EVALUASI KEAMANAN INFORMASI BERBASIS INDEKS KAMI

INDEKS KAMI

- Indeks KAMI adalah alat evaluasi untuk **menganalisis tingkat kesiapan** pengamanan informasi di instansi pemerintah.
- Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan **gambaran kondisi kesiapan** (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi.
- Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2013.

AREA EVALUASI

- Kategori Sistem Elektronik yang digunakan Instansi
- Tata Kelola Keamanan Informasi
- Pengelolaan Risiko Keamanan Informasi
- Kerangka Kerja Keamanan Informasi
- Pengelolaan Aset Informasi
- Teknologi dan Keamanan Informasi

Kategori Sistem Elektronik

- Definisi kategori sistem elektronik bisa dijabarkan untuk tingkat Satuan Kerja baik di tingkat Kementerian/Lembaga, ataupun untuk satuan kerja yang lebih kecil, sampai ke Unit Eselon III.
- Kategorisasi Sistem Elektronik:
  - Rendah
  - Tinggi
  - Strategis

Pengelompokan Pertanyaan

Pertanyaan dikelompokkan untuk 2 keperluan:

- Pengelompokan 1 berdasarkan **tingkat kesiapan** penerapan pengamanan sesuai dengan **kelengkapan kontrol** yang diminta oleh standar ISO/IEC 27001:2013.
  - Label “1” -> kerangka kerja dasar (*pertanyaan no.1-8*)
  - Label “2” -> efektivitas dan konsistensi penerapan (*pertanyaan no.9-16*)
  - Label “3” -> kemampuan peningkatan kinerja (*pertanyaan no.17-22*)

Pengelompokan Pertanyaan

Pertanyaan dikelompokkan untuk 2 keperluan:

- Pengelompokan 2 berdasarkan **tingkat kematangan** penerapan pengamanan dengan kategorisasi yang mengacu pada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT atau CMMI. Tingkat kematangan ini digunakan sebagai alat untuk melaporkan pemetaan dan **pemeringkatan kesiapan** keamanan informasi di instansi.
  - Tingkat I – Kondisi Awal
  - Tingkat II – Penerapan Kerangka Kerja Dasar
  - Tingkat III – Terdefinisi dan Konsisten
  - Tingkat IV – Terkelola dan Terukur
  - Tingkat V – Optimal
- Sebagai padanan terhadap standar ISO/IEC 2700:2013, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.

Hasil Evaluasi

Indeks KAMI (Keamanan Informasi)

Responden:
Satuan Kerja
Direktorat
Departemen

Alamat 1
Alamat 2
Kota Kode Pos

(Kode Area) Nomor Telpon
user@departemen_responden.go.id
HH/BB/TTTT

Hasil Evaluasi:

Tingkat Kematangan — I | I+

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Peran — 260

Peran/Tingkat Kepentingan TIK	: 31	Tingkat Ketergatungan:	Tinggi
Tata Kelola	: 35	Tingkat Kematangan: I+	
Pengelolaan Risiko	: 33	Tingkat Kematangan: I+	I+
Kerangka Kerja Keamanan Informasi	: 52	Tingkat Kematangan: II	s/d
Pengelolaan Aset	: 71	Tingkat Kematangan: I+	II+
Teknologi dan Keamanan Informasi	: 69	Tingkat Kematangan: II+	

Implementasi

- Indeks KAMI sebaiknya digunakan 2X dalam setahun sebagai alat untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu.

DISKUSI & TANYA JAWAB