



DIGITAL
TALENT
SCHOLARSHIP



pengantar standar Sistem manajemen KEAMANAN INFORMASI ISO/IEC 27001:2013



KOMINFO



#JADIJAGOANDIGITAL

Badan Penelitian dan Pengembangan Sumber Daya Manusia

Tujuan Pembelajaran

Setelah mengikuti pelatihan modul ini, peserta diharapkan mengenal standar dan memahami keuntung menerapkan standar Manajemen Keamanan Informasi.



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. Sesuatu yang memberikan **gambaran "mutu"**
10. **Perbaikan terus** (Continuous improvement)-hari ini "lebih baik dari hari lain"
11. Kesepatan berbasis **musyawarah** dengan menindahkan agama budaya lingkungan kerarifan lokal IPTEK

Mengapa perlu standar ? (Cont.)

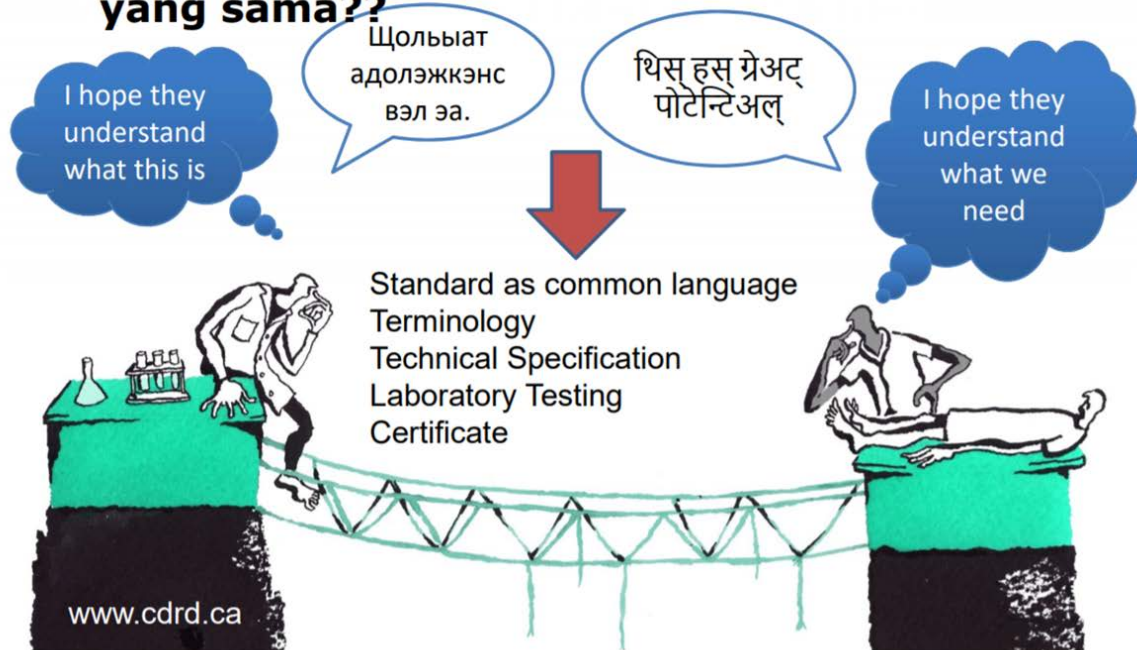
- Melindungi konsumen, pelaku usaha dan masyarakat
- Meningkatkan jaminan mutu, efisiensi produksi, dan kemampuan pelaku usaha
- Bahasa dalam semua bidang, baik perdagangan, industri, pendidikan, dan pengujian
- Meningkatkan kepastian dan efisiensi transaksi perdagangan barang dan jasa baik dalam negeri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



Dan lain-lain

Kenapa kita tidak menggunakan bahasa yang sama??

Standard
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**;



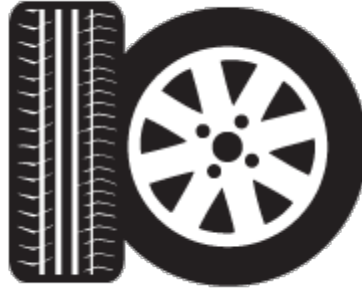
Meningkatkan perlindungan kepada konsumen,

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.

Cont oh Standar



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.

”

(Klausul 3.1.9)

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 kritis bagi operasional organisasi.
- ✓ Informasi 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



Aset tidak Berwujud : Reputasi, Image Perusahaan

Apa itu Keamanan Informasi?


“

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

- SNI ISO/IEC 27001:2013 -

”

SNI ISO/IEC 27001:2013

- 
- Adalah satu-satunya sistem manajemen keamanan informasi (SMKI) yang berstandar internasional.
 - *Auditable*
 - Mengadopsi pendekatan P-D-C-A
 - Berbasis Analisis Risiko dengan 114 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

Elemen Keamanan Informasi

Confidentiality



Integrity



Avallability



SNI ISO/IEC 27001:2013
Sistem Manajemen Keamanan
Informasi (SMKI)

Process



Technology



People

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.



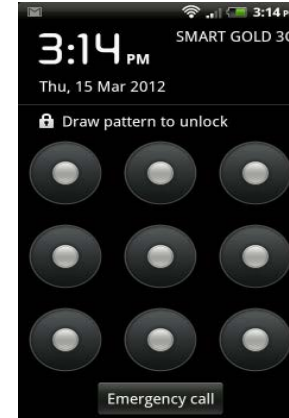
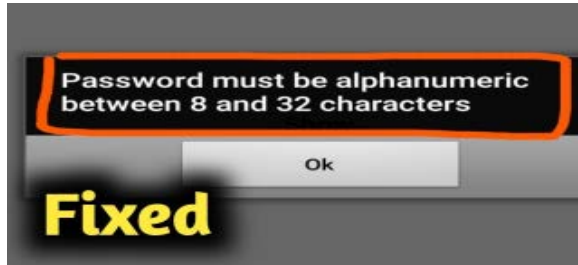
Kabel, Perangkat dan Jaringan Data/Voice, Layanan Telekomunikasi (Video Conferencing), Server, Desktop & Media Penyimpanan, Sistem Operasi, Aplikasi, dll.

Video Awareness

User Tidak Aware SMKI



Bentuk Pengamanan SMKI



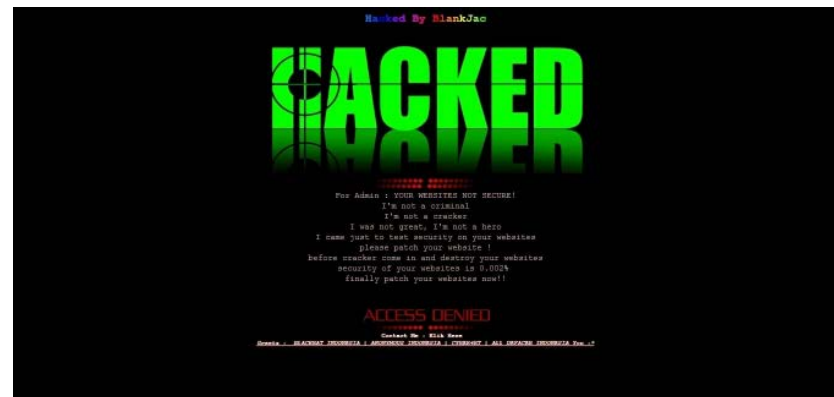
Session Expired
Please log in again.

OK



Serangan Keamanan Informasi

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



Motivasi Dibalik Serangan Cyber



Hanya untuk
bersenang-senang



Ketenaran dan
popularitas



Kegiatan yang
menantang



Keuntungan finansial
pribadi



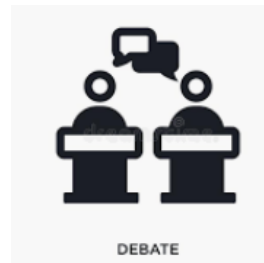
Kecemburuan,
kemarahan



Balas dendam



Serangan acak



Ideologis / politis

Dampak Risiko

Reputasi



REPUTATION GRAPHIC

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**.



Apa itu SNI ISO/IEC 27001:2013

- Adalah satu-satunya sistem manajemen keamanan informasi (SMKI) yang berstandar internasional.
- *Auditable*
- Mengadopsi pendekatan **P-D-C-A**.
- Berbasis Analisis Risiko dengan 114 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%



Siapa Yang membutuhkan ? SNI ISO/IEC 27001:2013



Manfaat menerapkan SMKI



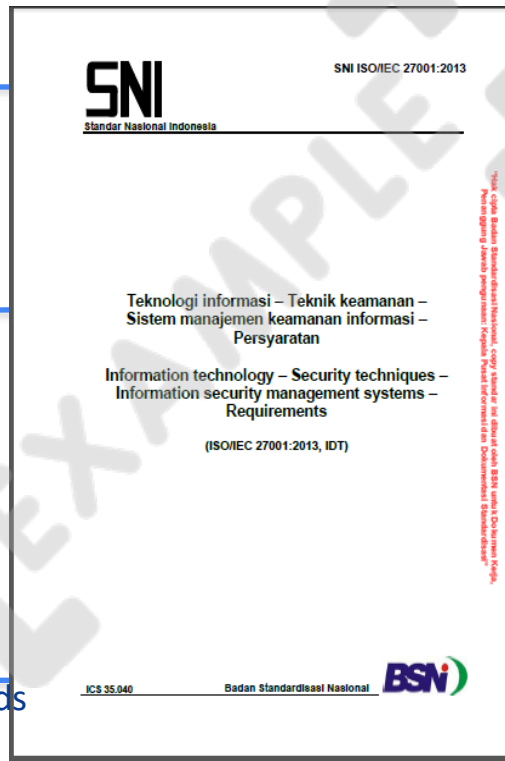
- Mengidentifikasi tujuan keamanan informasi
- Melindungi sumberdaya informasi dari gangguan keamanan informasi
- Mempelajari tentang tanggungjawab personil untuk menjaga keamanan informasi
- Merespon insiden keamanan informasi apabila mengalami masalah keamanan informasi.

SNI ISO/IEC 27001:2013

Logo Dokumen
SNI

Judul SNI

Kode International
Classification Standards



Nomor SNI

Watermark

Logo BSN

SNI ISO/IEC 27001:2013

ISO 27000 Family of International Standards

Provides the best practice recommendations on InfoSec management, risks and controls within the context of an overall ISMS.

ISO 27000: Overview and Vocabulary (2014)

ISO 27001: ISMS Requirements (2013)

ISO 27002: Code of Practice (2013)

ISO 27003: ISMS Implementation Guidance (2010)

ISO 27004: ISM Measurement (2009)

ISO 27005: InfoSec Risk Management (2011)

ISO 27006: Requirements for Bodies Providing Audit and Certification of ISMS (2011)

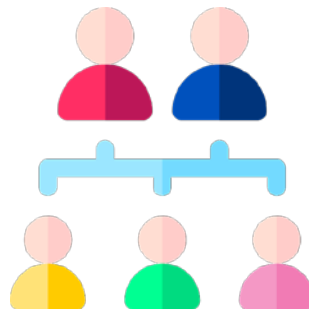
ISO 27007 – 27008: Guidelines for Auditing InfoSec Controls (2011)

ISO 27014: Governance of InfoSec (2013)

ISO 27015: ISM Guidelines for Financial Services (2012)

- www.iso.org

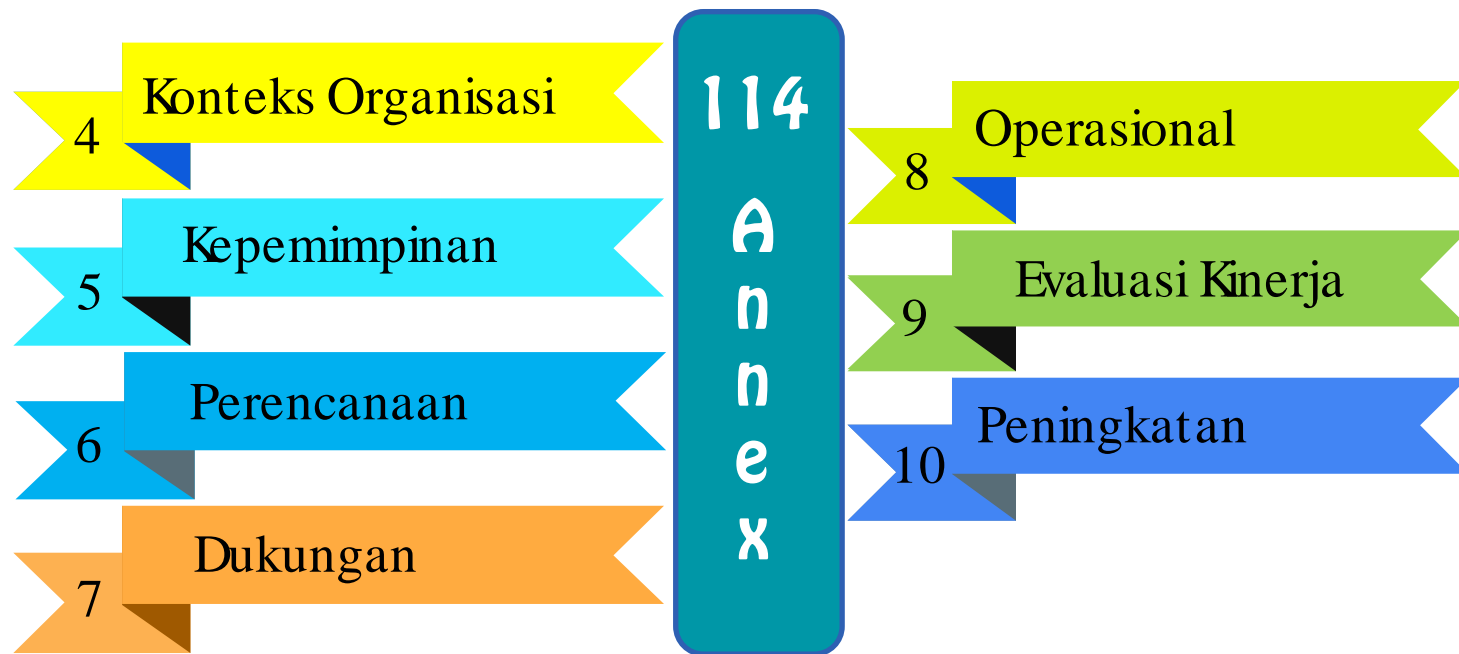
Keluarga ISO/IEC 27001:2013



Struktur SNI ISO/ISO 27001:2013

Klausul : Ketentuan (7)

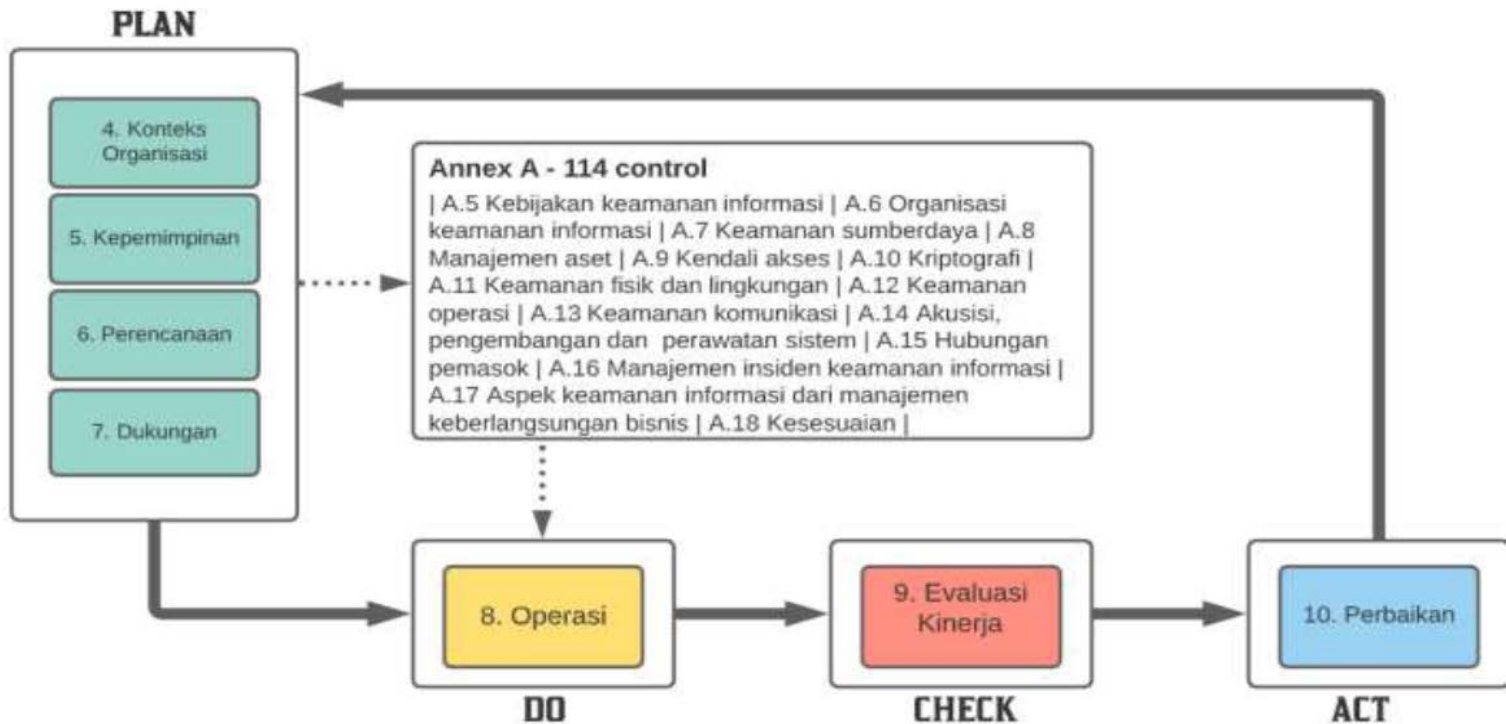
Annex: Titik Kendali, Titik Kritis, Persyaratan (114)



Struktur SNI ISO/IEC 27001:2013



Siklus PDCA SNI ISO/IEC 27001:2013



Lampiran Annex SNI ISO/IEC 27001:2013

SNI ISO/IEC 27001:2013

Lampiran A (normatif) Acuan untuk sasaran kendali dan kendali

Sasaran kendali dan kendali yang tercantum dalam Tabel A.1 secara langsung berasal dari dan sesuai dengan yang terdaftar di ISO/IEC 27002:2013[1], Klausul 5 hingga klausul 18, dan akan dipergunakan dalam Klausul 8.1.3.

Tabel A.1 — Sasaran kendali dan kendali

A.5 Kebijakan keamanan informasi	
A.5.1 Arahan manajemen untuk keamanan informasi	
Sasaran: Untuk memberikan arah dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan regulasi dan hukum yang relevan	
A.5.1.1	<div> <div>Kebijakan untuk keamanan informasi</div> <div><i>Kendali</i> Seperangkat kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak luar yang terkait.</div> </div>
A.5.1.2	<div> <div>Reviu kebijakan keamanan informasi</div> <div><i>Kendali</i> Kebijakan untuk keamanan informasi harus direviu pada interval waktu terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan dan keefektifan yang berkelanjutan</div> </div>
A.6 Organisasi keamanan informasi	
A.6.1 Organisasi internal	
Sasaran: Untuk membentuk kerangka kerja manajemen untuk memulai dan mengendalikan implementasi dan operasi keamanan informasi dalam organisasi.	
A.6.1.1	<div> <div>Peran dan tanggung jawab keamanan informasi</div> <div><i>Kendali</i> Semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan.</div> </div>
A.6.1.2	<div> <div>Pemisahan tugas</div> <div><i>Kendali</i> 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.</div> </div>
A.6.1.3	<div> <div>Hubungan dengan pihak berwenang</div> <div><i>Kendali</i> Hubungan baik dengan pihak berwenang terkait harus dipelihara.</div> </div>
A.6.1.4	<div> <div>Hubungan dengan kelompok minat khusus</div> <div><i>Kendali</i> Hubungan baik dengan komunitas, forum, dan asosiasi profesional spesialis keamanan harus dipelihara.</div> </div>

SNI ISO/IEC 27001:2013

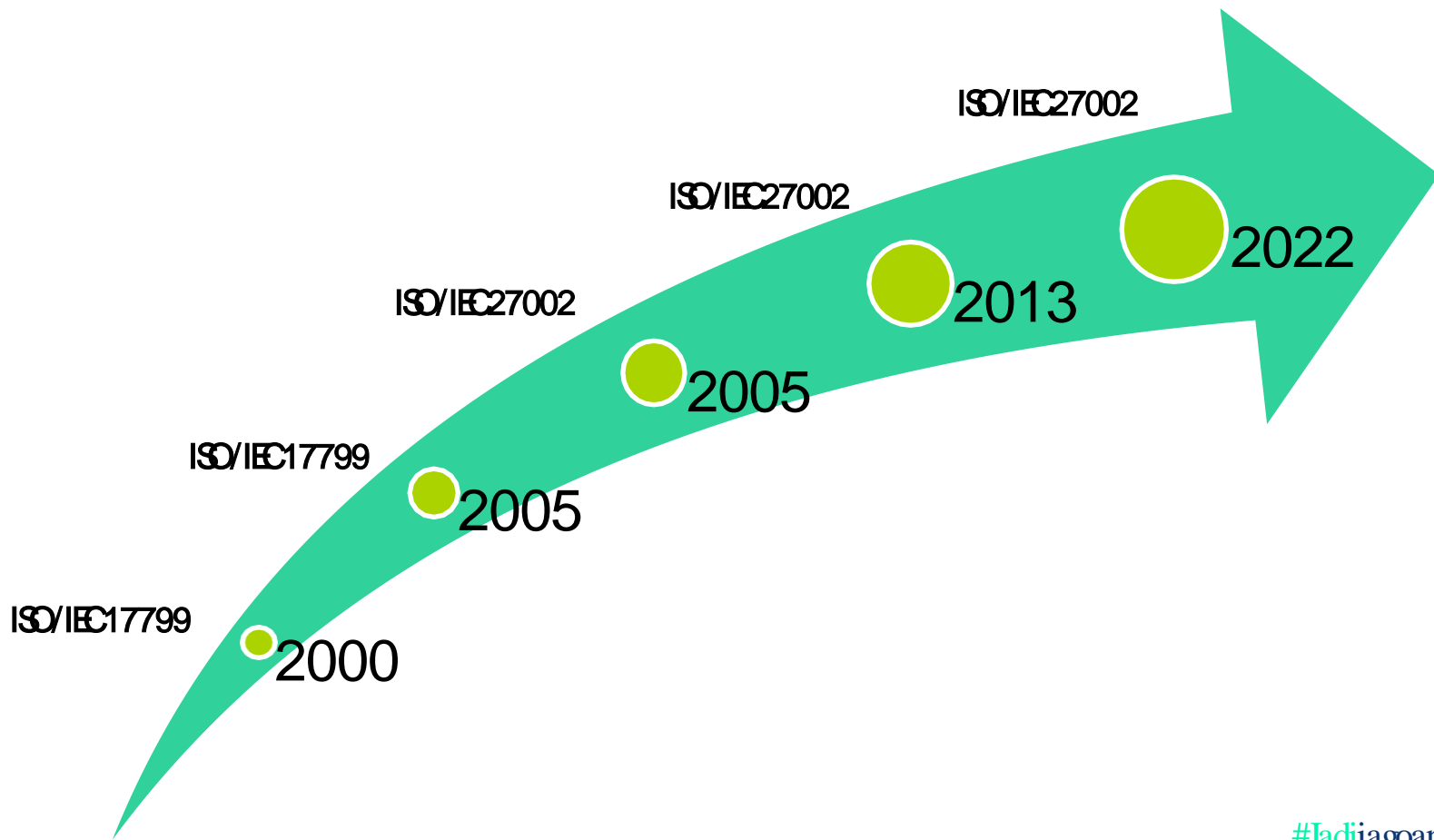
Tabel A.1 - (lanjutan)

A.6.1.5	<div> <div>Keamanan informasi dalam manajemen proyek</div> <div><i>Kendali</i> Keamanan informasi harus diterapkan ke dalam manajemen proyek, tanpa memperhatikan tipe proyeknya.</div> </div>	<div> <div>Keamanan informasi harus diterapkan ke dalam manajemen proyek, tanpa memperhatikan tipe proyeknya.</div> </div>
A.6.2 Perangkat bergerak (mobile device) dan teleworking		
Sasaran: Untuk menjamin keamanan teleworking dan penggunaan perangkat bergerak		
A.6.2.1	<div> <div>Kebijakan perangkat bergerak</div> <div><i>Kendali</i> Kebijakan dan tindakan keamanan yang mendukung harus diadopsi untuk mengelola risiko yang terjadi akibat dari penggunaan perangkat bergerak.</div> </div>	
A.6.2.2	<div> <div>Teleworking</div> <div><i>Kendali</i> Kebijakan dan tindakan keamanan yang mendukung harus diimplementasikan untuk melindungi informasi yang diakses, diproses atau disimpan di dalam situs teleworking.</div> </div>	
A.7 Keamanan sumber daya manusia		
A.7.1 Sebelum dipekerjakan		
Sasaran: Untuk memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka dan sesuai dengan peran yang ditetapkan bagi mereka.		
A.7.1.1	<div> <div>Penyaringan</div> <div><i>Kendali</i> Verifikasi latar belakang dari semua calon pegawai harus dilaksanakan berdasarkan hukum, regulasi dan etika terkait dan harus proporsional terhadap persyaratan bisnis, klasifikasi informasi yang akan diakses, dan risiko yang dipersepsikan.</div> </div>	
A.7.1.2	<div> <div>Syarat dan ketentuan kepegawaian</div> <div><i>Kendali</i> Perjanjian tertulis dengan pegawai dan kontraktor harus menyatakan tanggung jawab keamanan informasi mereka dan organisasi.</div> </div>	
A.7.2 Selama bekerja		
Sasaran: Untuk memastikan bahwa pegawai dan kontraktor menyadari dan memenuhi tanggung jawab keamanan informasi mereka		
A.7.2.1	<div> <div>Tanggung jawab manajemen</div> <div><i>Kendali</i> Manajemen harus mewajibkan semua pegawai dan kontraktor menerapkan keamanan informasi berdasarkan kebijakan dan prosedur organisasi yang sudah ditetapkan.</div> </div>	
A.7.2.2	<div> <div>Kepedulian, pendidikan, dan pelatihan keamanan informasi</div> <div><i>Kendali</i> Semua pegawai organisasi dan kontraktor (jika relevan) harus menerima kepedulian, pendidikan, dan pelatihan yang memadai dan pemberitahuan secara berkala mengenai kebijakan dan prosedur organisasi, sesuai dengan fungsi kerja mereka.</div> </div>	

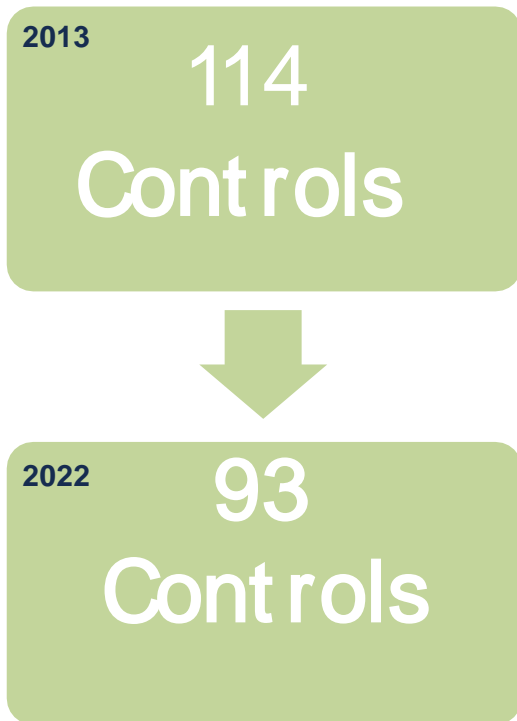
Lampiran Annex SNI ISO/IEC 27001:2013

SNI ISO/IEC 27001:2013 Control Point and Control Objective		
Annex	Deskripsi	total Kontrol
A5	Kebijakan Keamanan Informasi	2
A6	Organisasi Keamanan informasi	7
A7	Keamanan Sumber Daya Manusia	6
A8	Manajemen Aset	10
A9	Kendali Akses	14
A10	Kriptografi	2
A11	Keamanan Fisik dan Lingkungan	15
A12	Keamanan Operasi	14
A13	Keamanan Komunukasi	7
A14	Akuisisi, Pengembangan dan Perawatan Sistem	13
A15	Hubungan Pemasok	5
A16	Manajemen Insiden Keamanan Informasi	7
A17	Aspek Keamanan Informasi dari Manajemen Keberlangsungan	4
A18	Kesesuaian	8
Total Kontrol		114

SNI ISO/IEC 27002:2022 ?



SNI ISO/IEC 27002:2022 ?



ISO/IEC 27001 Annex A will be updated on new revision

Statement of Applicability (SOA)

Statement of Applicability (SoA)



Dokumentasi Analisis Kontrol Implementasi SMKI



Pernyataan Kontrol terhadap Annex A ISO 27001:2013



14 Domain & 114 Kontrol Pengamanan Informasi

Statement of Applicability (SOA)

Pernyataan Penerapan

Tanda (untuk Pemilihan Kontrol dan Alasan Pemilihan Kontrol)

PH: Persyaratan Hukum, KK: Kewajiban Kontrak, PB/BP: Persyaratan Bisnis/Best Practice, HPR: Hasil Penilaian Risiko, SBT: Sampai Batas Tertentu

Kontrol ISO/IEC 27001:2013			Kontrol saat ini	Catatan Pengecualian	Pemilihan kontrol dan alasan pemilihan				Catatan Penerapan
Clause	Sec	Sasaran Kontrol			PH	KK	PB/BP	HPR	
4 Konteks Organisasi	4,1	Konteks Organisasi untuk Keamanan Informasi							
	4.1.1	Identifikasi isu internal dan eksternal	Sudah					√	
	4.1.2	Kebutuhan dan ekspektasi Keamanan Informasi	Sudah					√	
	4.1.3	Ruang Lingkup Keamanan Informasi	Sudah					√	
5 Kebijakan Keamanan Informasi	5,2	Arahan Manajemen untuk Keamanan Informasi							
	5.2.1	Kebijakan untuk Keamanan Informasi	Sudah		√				
	5.2.2	Review Kebijakan Keamanan Informasi	Belum			√			
	5,3	Organisasi Internal							
	5.3.1	Aturan Keamanan Informasi dan Tanggung Jawab	Sudah		√				
	5.3.2	Pemisahan Tugas	Sudah				√		
	5.3.3	Hubungan dengan Otoritas	Partial				√		
	5.3.4	Hubungan dengan Unit terkait	Partial				√		
	5.3.5	Keamanan Informasi dalam Manajemen Proyek	Partial			√			

Sekilas Tahapan Implementasi SMKI



Contoh Sertifikat SNI ISO/IEC 27001:2013



CERTIFICATE

Certificate No. [REDACTED]

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) [REDACTED]

(Alamat Instansi/Lembaga/Organisasi) [REDACTED]

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

Keuntungan menerapkan SNI ISO/IEC 27001:2013

- ✓ 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 27001:2013

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



#Jadijagoandigital
TerimaKasih



digitalent.kominfo



DTS_kominfo



digitalent.kominfo



digital talent scholarship