



KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA



BADAN
STANDARDISASI
NASIONAL



Pengenalan SNI ISO/IEC 27001:2013 Sistem Manajemen Keamanan Informasi

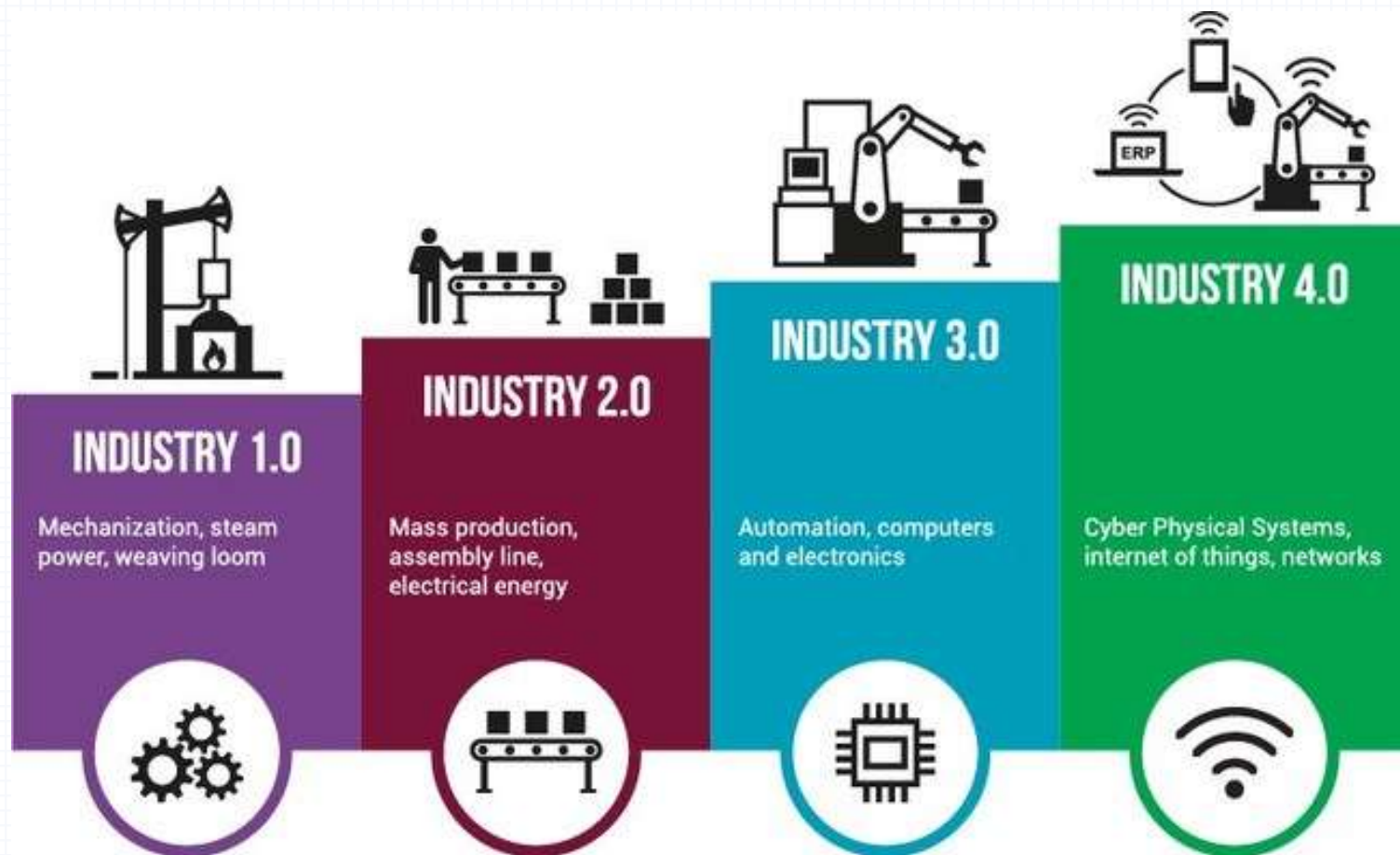
Jakarta, 21 Juli 2020

Akbar Aryanto

Tim Manajemen Resiko SPBE

Kepala Bidang Infrastruktur dan Keamanan Informasi - BSN

Jakarta, 21 Juli 2020





KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA



BADAN
STANDARDISASI
NASIONAL

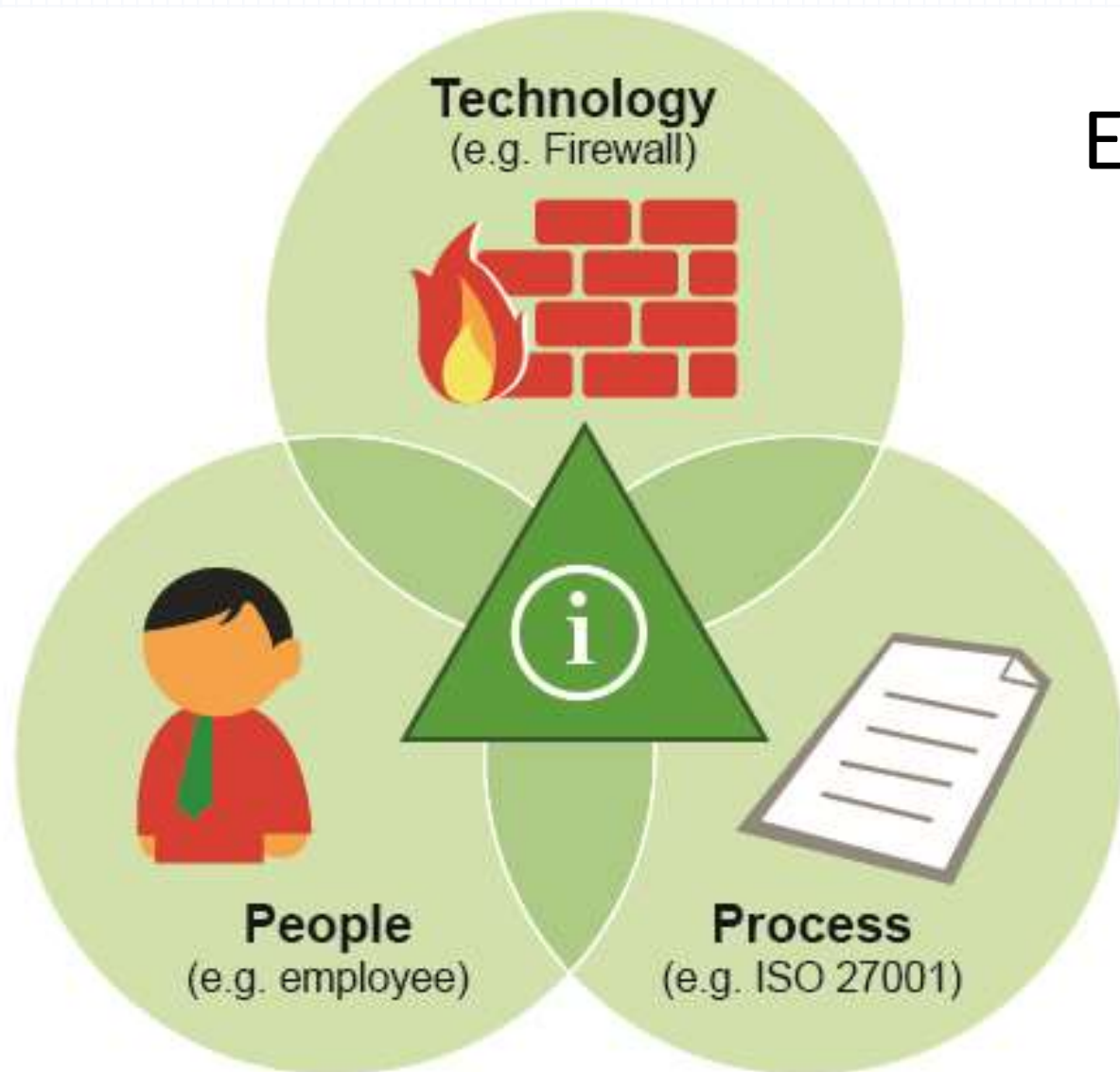


Teknologi Informasi





Elemen Keamanan Informasi





KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA



**BADAN
STANDARDISASI
NASIONAL**





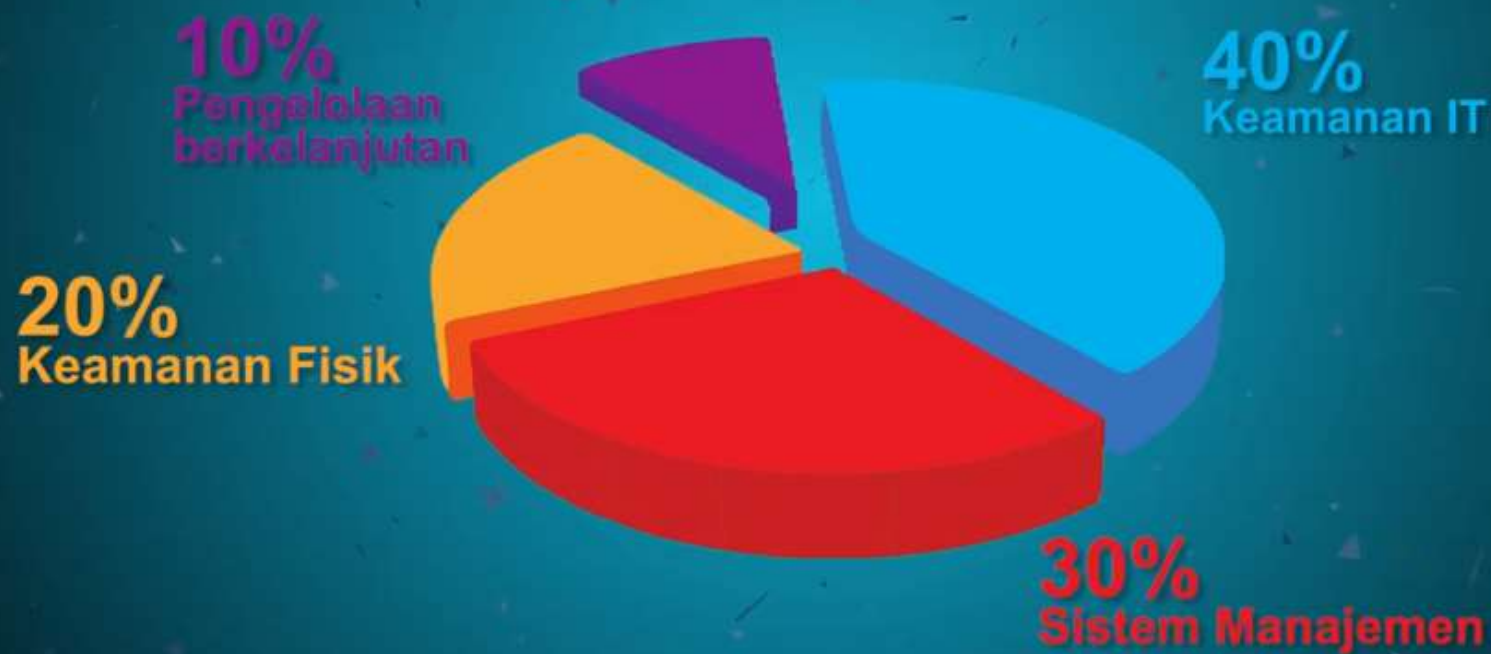
SNI ISO/IEC 27001:2013

Sistem Manajemen Keamanan Informasi (SMKI)





Komposisi Standar Manajemen Keamanan Informasi





Apa itu Keamanan Informasi



“Keamanan Informasi **adalah** Penjagaan terhadap Kerahasiaan (**C**onfidentiality), Keutuhan (**I**ntegrity) dan Ketersediaan (**A**vailability) atas informasi. ”

- SNI ISO/IEC 27000:2013 -





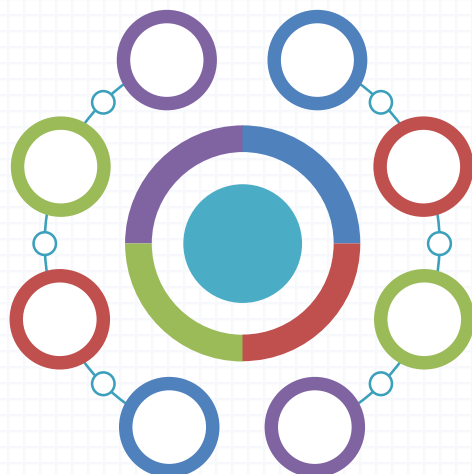
Konsep Utama SMKI





Struktur

SNI ISO/IEC 27001:2013



Terdiri dari 10 klausul dan lampiran Annex, dengan 14 Kelompok Domain dan 114 Kendali (Kontrol)

Klausul 4 - 10 tidak dapat dikecualikan (wajib) dalam sertifikasi SNI ISO/IEC 27001:2013

1. Ruang Lingkup

2. Acuan Normatif

3. Istilah dan Definisi

4. Konteks Organisasi

- 4.1 Memahami organisasi & kontek
- 4.2 Memahami kebutuhan
- 4.3 Penentuan ruang lingkup SMKI
- 4.4 SMKI

5. Kepemimpinan

- 5.1 Kepemimpinan & komitmen
- 5.2 Kebijakan
- 5.3 Peran organisasi, tanggung jawab & wewenang

6. Perencanaan

- 6.1 Tindakan untuk menangani resiko & peluang
- 6.2 Sasaran keamanan informasi & perencanaan untuk mencapainya

7. Dukungan

- 7.1 Sumberdaya
- 7.2 Kompetensi
- 7.3 Kepedulian
- 7.4 Komunikasi
- 7.5 Informasi terdokumentasi

8. Operasi

- 8.1 Perencanaan & pengendalian operasional
- 8.2 Penilaian resiko keamanan informasi
- 8.3 Penanganan resiko keamanan informasi

9. Evaluasi Kinerja

- 9.1 Pemantauan, pengukuran, analisis & evaluasi
- 9.2 Audit internal
- 9.3 Reviu manajemen

10. Perbaikan

- 10.1 Ketidaksesuaian & tindakan korektif
- 10.2 Perbaikan berkelanjutan



Klausul wajib

SNI ISO/IEC 27001:2013

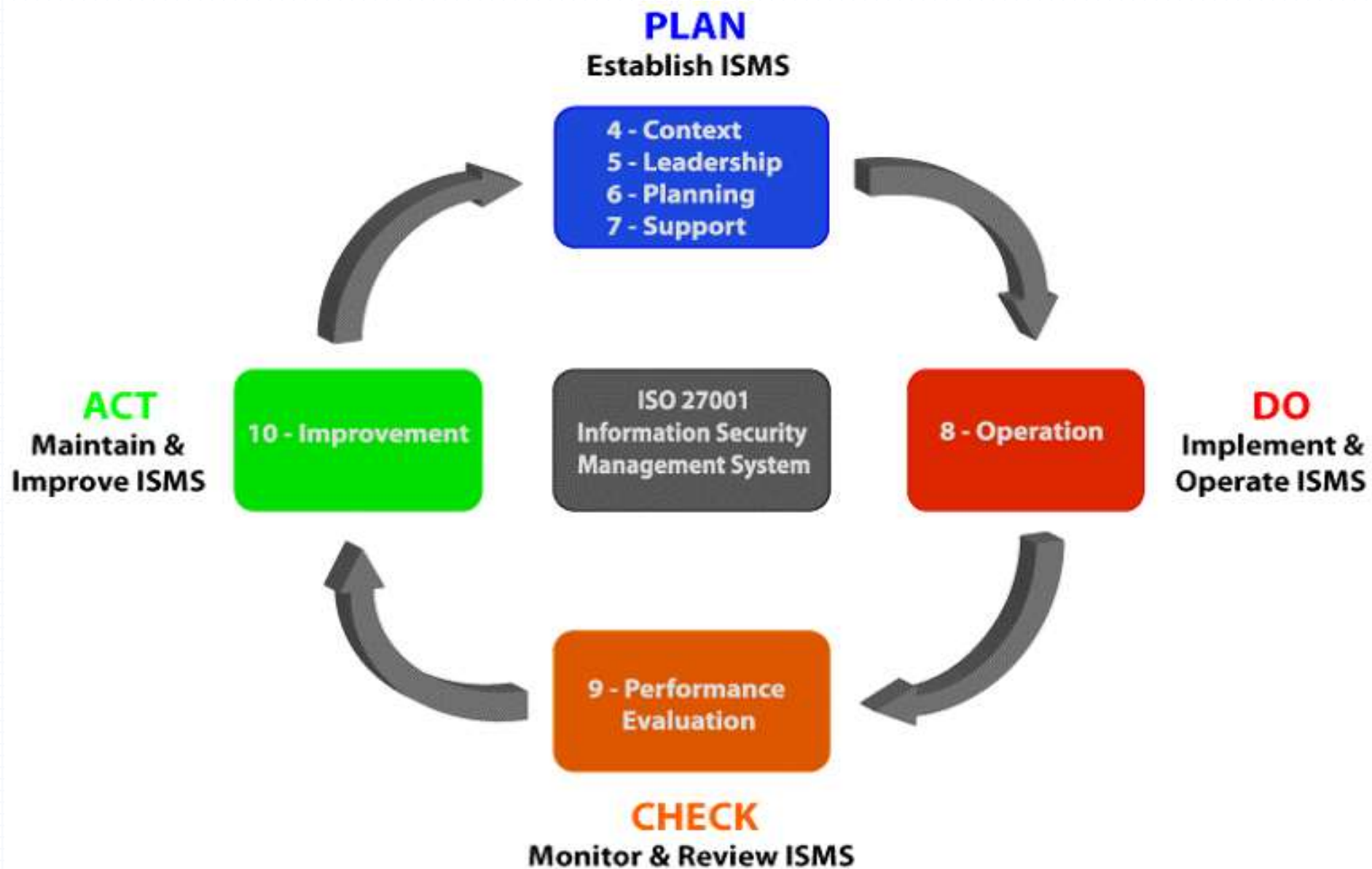




Klausul wajib

SNI ISO/IEC 27001:2013







Lampiran Anex 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



Contoh Kasus

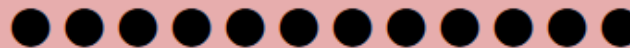






<https://howsecureismypassword.net/>

HOW SECURE IS MY PASSWORD?



It would take a computer about

4 WEEKS

to crack your password



Mengapa perlu SNI ISO/IEC 27001:2013 ?





Karena dengan menerapkan SMK...

- 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.





Keuntungan penerapan SNI ISO/IEC 27001:2013

- Melindungi, memelihara kerahasiaan, integritas dan ketersediaan informasi
- Mengelola serta mengendalikan resiko keamanan informasi
- Memberikan keyakinan dan jaminan kepada pelanggan
- Memastikan bahwa organisasi memiliki kontrol terkait keamanan informasi terhadap lingkungan proses bisnisnya yang mungkin menimbulkan risiko atau gangguan.
- Membuat pengaruh positif dalam hal citra perusahaan, nilai, dan persepsi yang baik dari pihak lain, dengan meminimalkan resiko sd level yang dapat diterima
- Membantu organisasi dalam menjalankan perbaikan dalam keamanan informasi
- Salah satu standar pengamanan informasi yang diakui di seluruh dunia.
- Patuh terhadap hukum dan undang-undang seperti UU ITE, dll.



Tahapan Implementasi SNI ISO 27001:2013





CERTIFICATE 

Certificate No. ISMS 00005

 **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@ucofindo.co.id

Menyatakan bahwa
Certify that

BADAN STANDARDISASI NASIONAL (BSN)
Gedung I BPPT
Jl. M.H. Thamrin No. 8, Jakarta Pusat - INDONESIA

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

Sertifikat ini berlaku dengan ketentuan bahwa organisasi selalu memenuhi kriteria
sebagaimana ditetapkan oleh SUCOFINDO INTERNATIONAL CERTIFICATION SERVICES
This certificate is valid provided that the organization continues to meet the criteria as
laid down by SUCOFINDO INTERNATIONAL CERTIFICATION SERVICES


Hertiana Dewi
Ketua Badan Pelaksana
Chairman of Governing Board

Sertifikat ini berlaku dari 21 Februari 2020 sampai 20 Februari 2023
This certificate is valid from February 21st, 2020 until February 20th, 2023


3445856
BCI-2007A

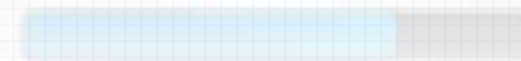


SUCCESS



LOADING...

LOADING...





KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA



**BADAN
STANDARDISASI
NASIONAL**

TERIMA KASIH