PDP pada SMKI

Chandra Yulistia – ISMSF.ID

27001 Day – 27 Januari 2023

ISMSF.ID

Perkenalan

Forum Sistem Manajemen Keamanan Informasi Indonesia

ISMSF.ID

Information Security Management System Forum Indonesia

- **Forum Sistem Manajemen Keamanan Informasi Indonesia** atau **Information Security Management System Forum Indonesia** yang disingkat **ISMSF.ID** adalah wadah untuk bertukar pikiran dan berbagi informasi secara bebas tentang keamanan informasi dalam rangka membangun sinergi kolaborasi mengamankan informasi di Indonesia.
- ISMSF.ID menyelenggarakan berbagai **kegiatan bertukar pikiran** di antara para praktisi, akademisi, dan regulator di bidang keamanan informasi. Kegiatan diadakan dalam bentuk diskusi, seminar, dan pelatihan baik secara daring maupun luring.
- ISMSF.ID menyelenggarakan berbagai **kegiatan berbagi informasi** terkait implementasi sistem manajemen keamanan informasi berdasarkan standar dan regulasi nasional dan global. Kegiatan diadakan dalam bentuk penyusunan kajian dan panduan terkait keamanan informasi.
- Informasi tentang ISMSF.ID dapat dilihat di situs https://ismsf.id atau hubungi ISMSF.ID melalui surel ke info [at] ismsf.id. Anda juga dapat mengikuti halaman Linkedin ISMSF.ID untuk informasi terkini.

Keamanan Informasi Buatan Indonesia

KIBI

Keamanan Informasi Buatan Indonesia (KIBI) atau *Information Security Made in Indonesia* adalah informasi tentang Barang dan Jasa di bidang Keamanan Informasi yang dihasilkan oleh pelaku industri Indonesia yang memenuhi persyaratan Produk Dalam Negeri.

Inisiatif ini didedikasikan sebagai bentuk partisipasi ISMSF.ID dalam mendukung Kampanye Pemerintah Indonesia tentang Peningkatan Penggunaan Produksi Dalam Negeri (P3DN).

Entri produk KIBI Anda di menu **Entri** atau lihat Daftar Produk KIBI di menu **Produk** tanpa dipungut biaya.

Silahkan kunjungi https://ISMSF.ID/KIBI

Kegiatan

ISMSF.ID

27 Januari 2022 :
1st International 27001 Day

22 Mei 2022
Diskusi 27002 dan 27001 versi 2022

27 Juli 2022
Introduksi SNI 27003 : Panduan SMKI 27001

27 Agustus 2022
Introduksi SNI 27004 : Evaluasi SMKI 27001

14 Desember 2022
Introduksi Revisi 27005:2022

27 Desember 2022
Transisi 27001:2022

14 Juni 2022 : FGD BSSN
Peluang Profesi Auditor dan Implementor SMKI

19 September 2022 : FGD BSSN
Evaluasi PBSSN 8/2020 SP-PSE

03 November 2022 : FGD BSSN
Identifikasi IIV

24 November 2022 : FGD BSSN
National Cyber Risk Assessment

27 Januari 2023
International 27001 Day

Chandra Yulistia

Pendidikan

- DIII STAN – Akuntansi
- S1 UNPAD – Akuntansi

Institusi

- 1996 – 2001: Auditor BPK RI
- 2002 – sekarang : Auditor & Konsultan pada beberapa perusahaan swasta

Sertifikasi Profesi

CISA CISM

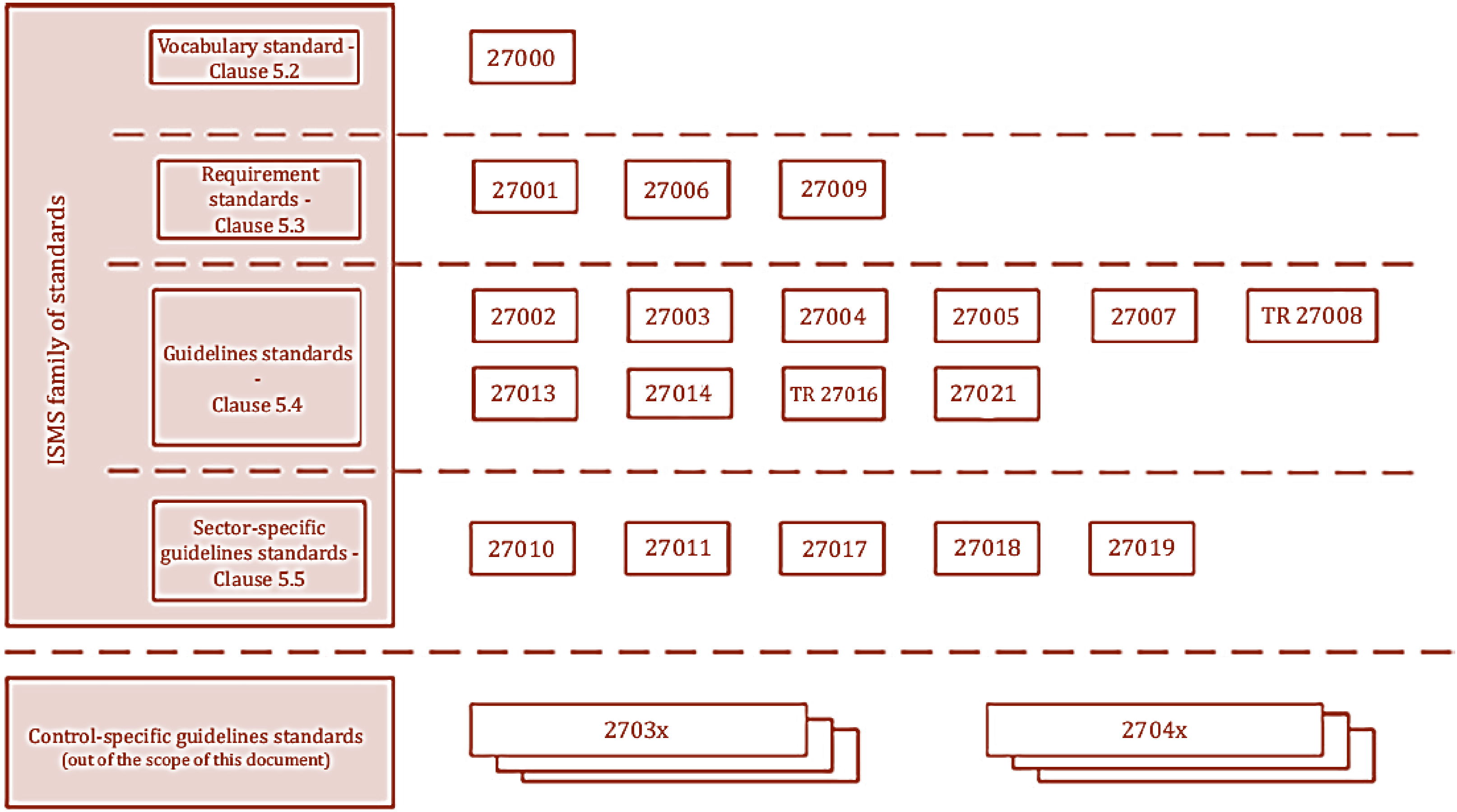
Asosiasi Profesi

- ISACA – Platinum Member
- IASII – Anggota Pendiri & Dewan Pengawas
- ISMS Forum Indonesia (ISMSF.ID) – Inisiator

- Komite Teknis 35-04 SNI Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi
    - Gugus Kerja SNI SMKI - Sistem Manajemen Keamanan Informasi
    - *Expert Member of WG1 & WG3 ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection*
- Komite Teknis 35-01 SNI Teknologi Informasi
    - Kelompok Kerja SNI Tata Kelola dan Manajemen Layanan TI
    - Kelompok Kerja SNI Pusat Data
    - Kelompok Kerja SNI Keamanan Informasi

27000

Seri 27000



ISMS family of standards

Vocabulary standard - Clause 5.2

27000

Requirement standards - Clause 5.3

27001 27006 27009

Guidelines standards - Clause 5.4

27002 27003 27004 27005 27007 TR 27008

27013 27014 TR 27016 27021

Sector-specific guidelines standards - Clause 5.5

27010 27011 27017 27018 27019

Control-specific guidelines standards (out of the scope of this document)

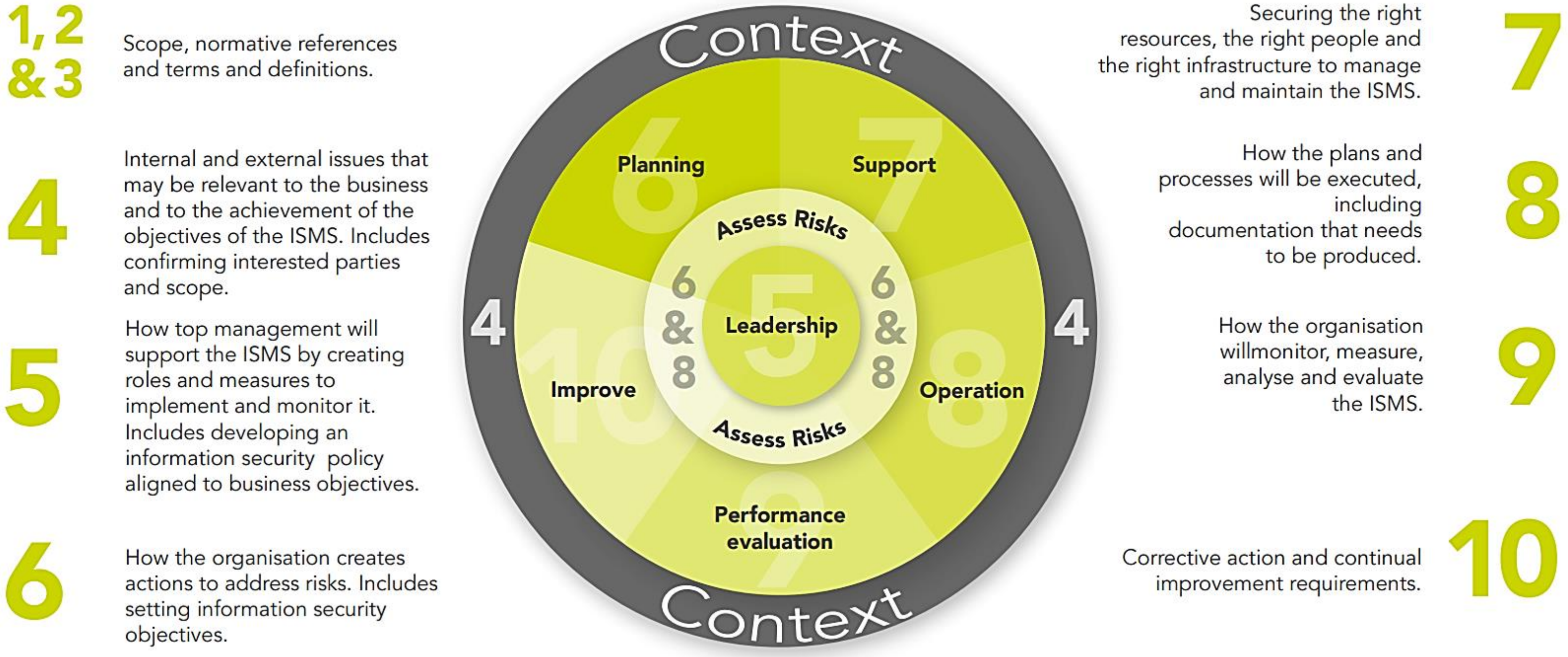
2703x

2704x

Sumber : ISO/IEC 27000:2018

27001

27001: 2022



1, 2 & 3 Scope, normative references and terms and definitions.

4 Internal and external issues that may be relevant to the business and to the achievement of the objectives of the ISMS. Includes confirming interested parties and scope.

5 How top management will support the ISMS by creating roles and measures to implement and monitor it. Includes developing an information security policy aligned to business objectives.

6 How the organisation creates actions to address risks. Includes setting information security objectives.

7 Securing the right resources, the right people and the right infrastructure to manage and maintain the ISMS.

8 How the plans and processes will be executed, including documentation that needs to be produced.

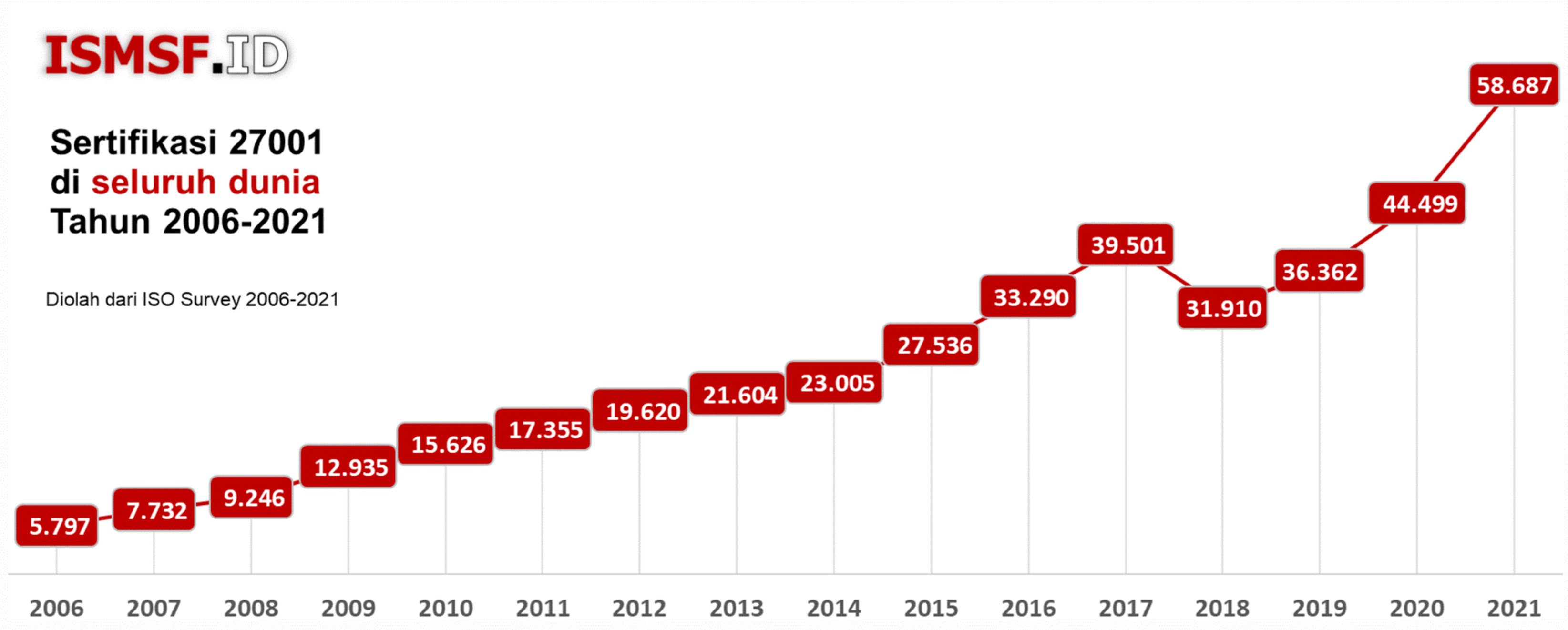
9 How the organisation willmonitor, measure, analyse and evaluate the ISMS.

10 Corrective action and continual improvement requirements.

Sumber : https://www.itgovernance.co.uk/iso27001

ISMSF.ID

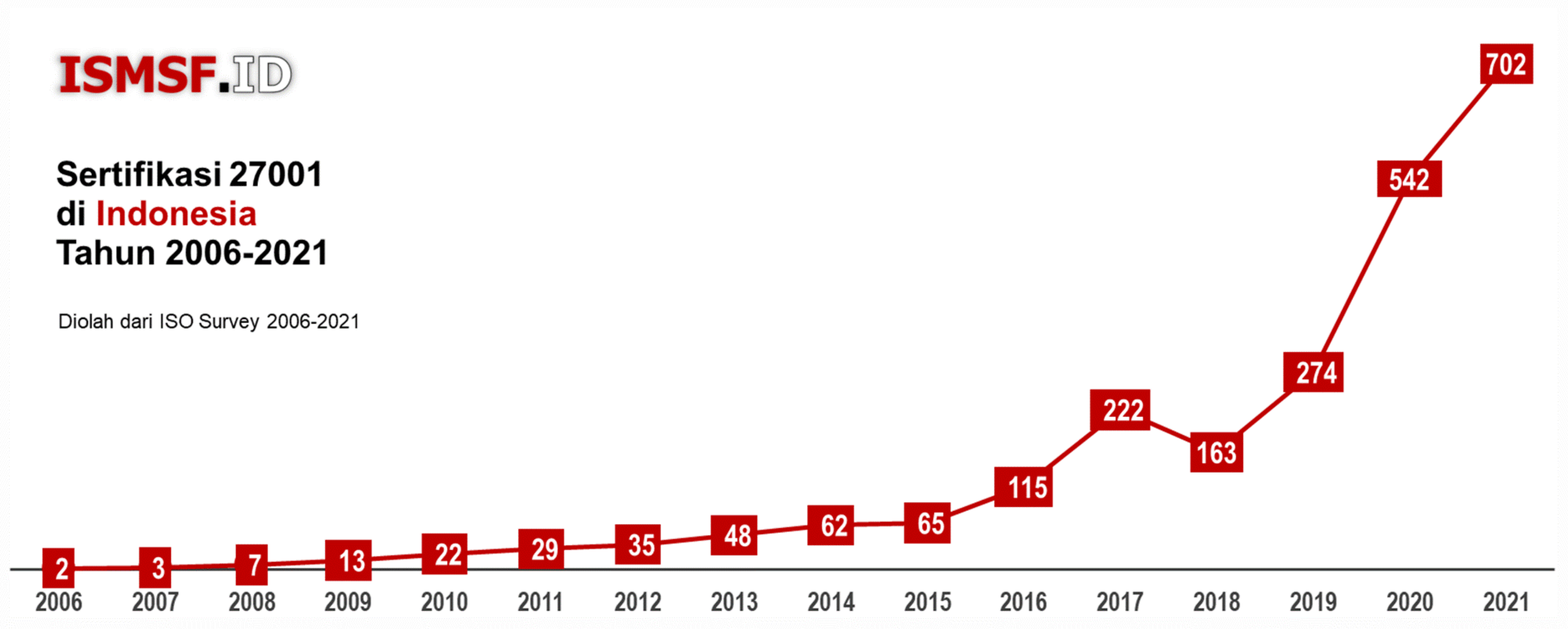
27001: 2022



Sertifikasi 27001
di seluruh dunia
Tahun 2006-2021

Diolah dari ISO Survey 2006-2021

27001: 2022



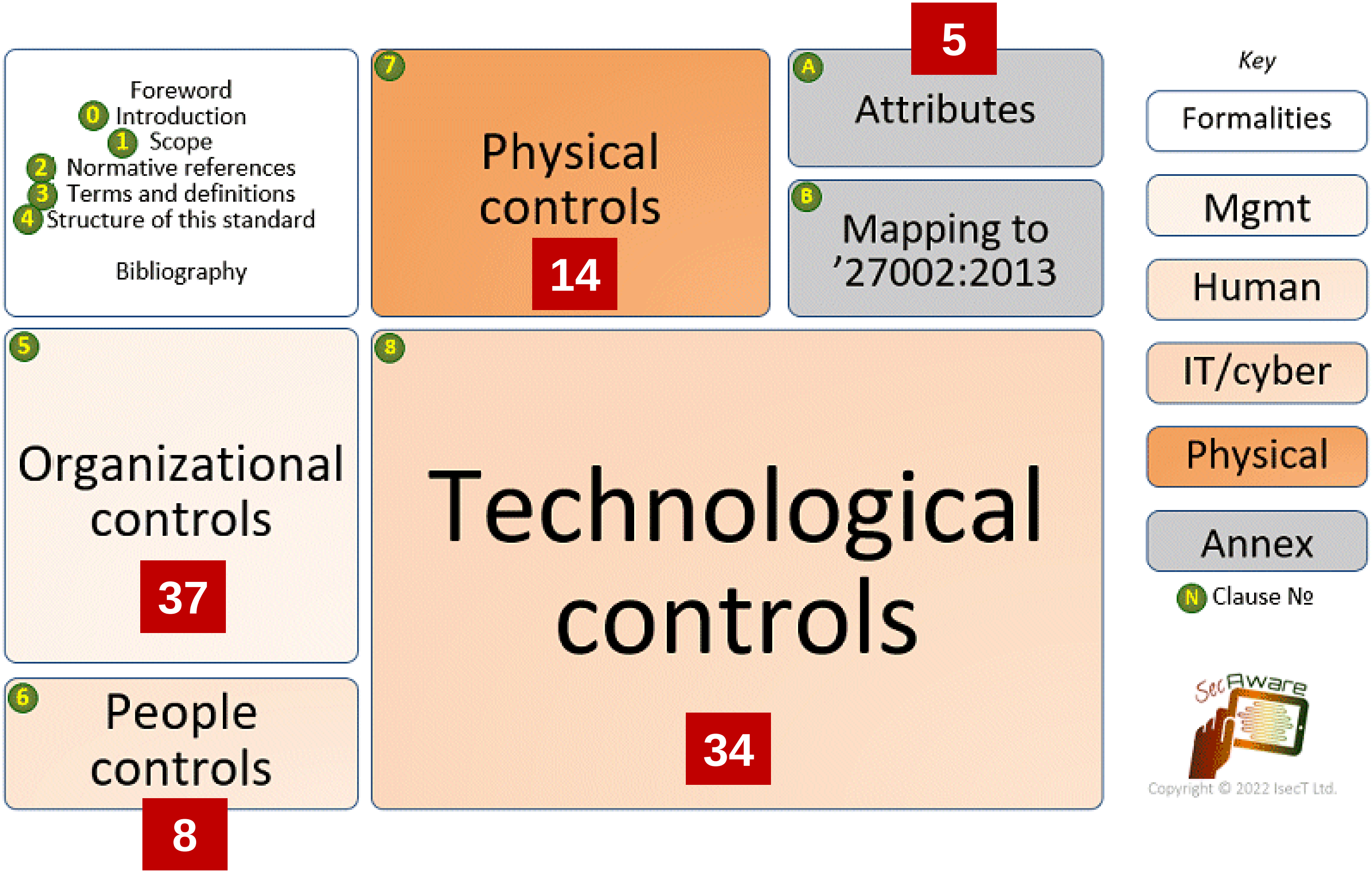
ISMSF.ID

Sertifikasi 27001
di Indonesia
Tahun 2006-2021

Diolah dari ISO Survey 2006-2021

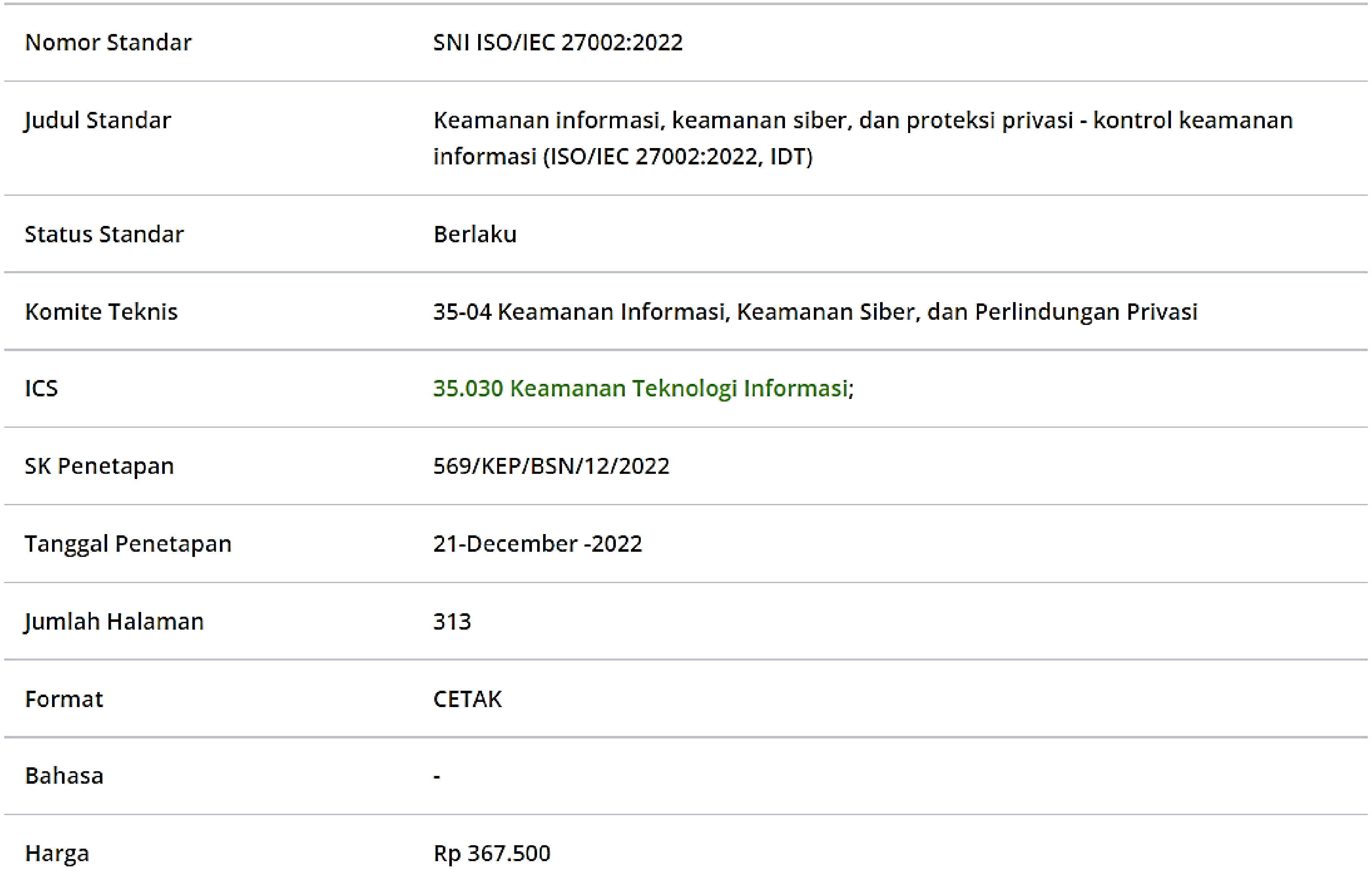
27002

27002: 2022



Sumber : https://www.iso27001security.com/html/27002.html

27002:2022



Nomor Standar	SNI ISO/IEC 27002:2022
Judul Standar	Keamanan informasi, keamanan siber, dan proteksi privasi - kontrol keamanan informasi (ISO/IEC 27002:2022, IDT)
Status Standar	Berlaku
Komite Teknis	35-04 Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi
ICS	35.030 Keamanan Teknologi Informasi;
SK Penetapan	569/KEP/BSN/12/2022
Tanggal Penetapan	21-December -2022
Jumlah Halaman	313
Format	CETAK
Bahasa	-
Harga	Rp 367.500

Sumber : https://pesta.bsn.go.id/produk/detail/14163-sniisoiec270022022

27701

27701: 2019

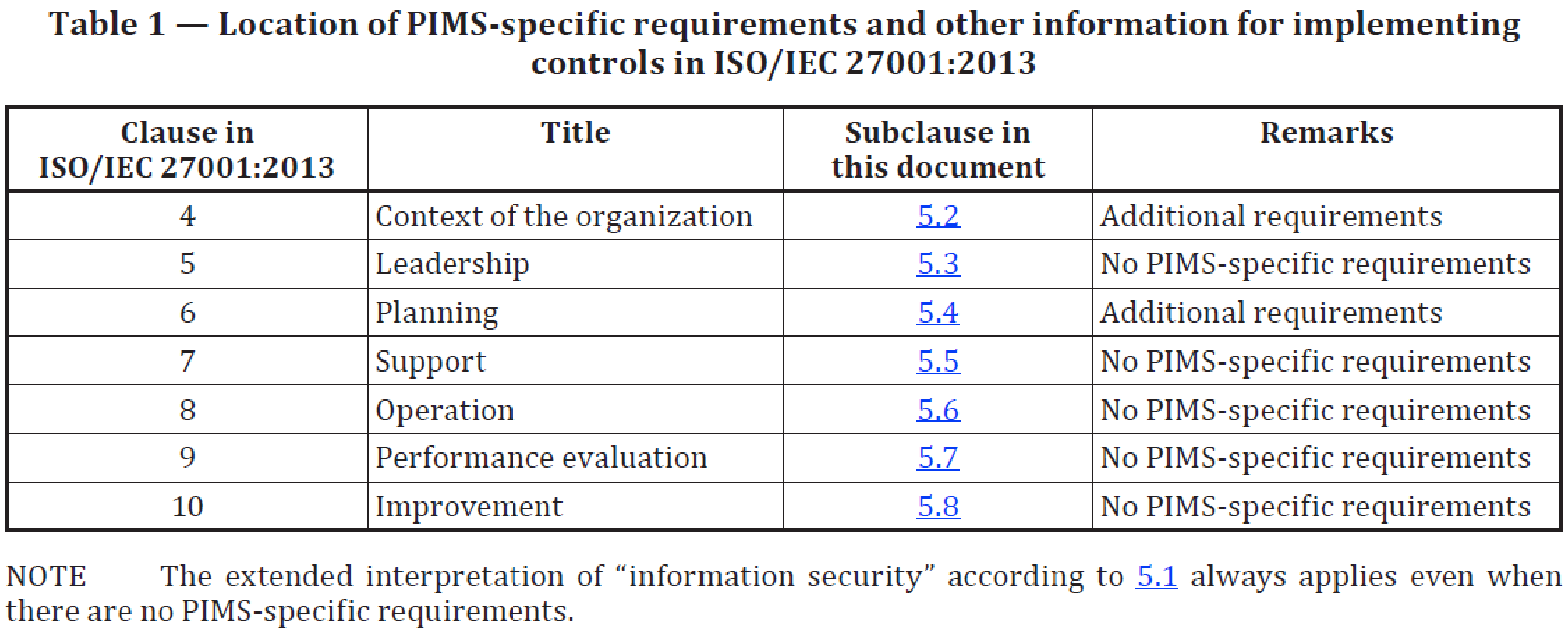


Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

Clause in ISO/IEC 27001:2013	Title	Subclause in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

NOTE The extended interpretation of "information security" according to 5.1 always applies even when there are no PIMS-specific requirements.

Sumber : SNI ISO/IEC 27701:2019

27701: 2019

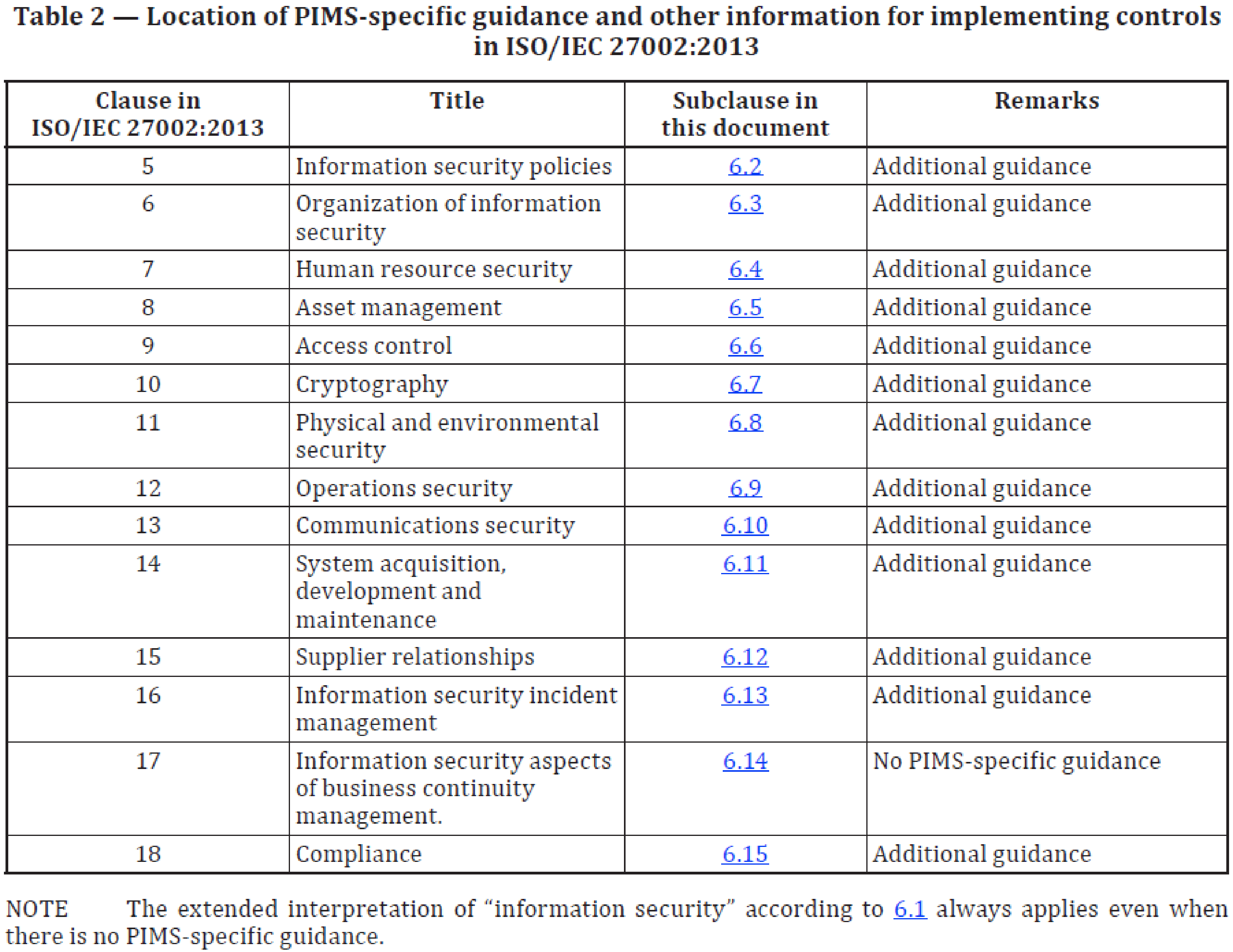


Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2013

Clause in ISO/IEC 27002:2013	Title	Subclause in this document	Remarks
5	Information security policies	6.2	Additional guidance
6	Organization of information security	6.3	Additional guidance
7	Human resource security	6.4	Additional guidance
8	Asset management	6.5	Additional guidance
9	Access control	6.6	Additional guidance
10	Cryptography	6.7	Additional guidance
11	Physical and environmental security	6.8	Additional guidance
12	Operations security	6.9	Additional guidance
13	Communications security	6.10	Additional guidance
14	System acquisition, development and maintenance	6.11	Additional guidance
15	Supplier relationships	6.12	Additional guidance
16	Information security incident management	6.13	Additional guidance
17	Information security aspects of business continuity management.	6.14	No PIMS-specific guidance
18	Compliance	6.15	Additional guidance

NOTE The extended interpretation of "information security" according to 6.1 always applies even when there is no PIMS-specific guidance.

Sumber : SNI ISO/IEC 27701:2019

27701: 2019

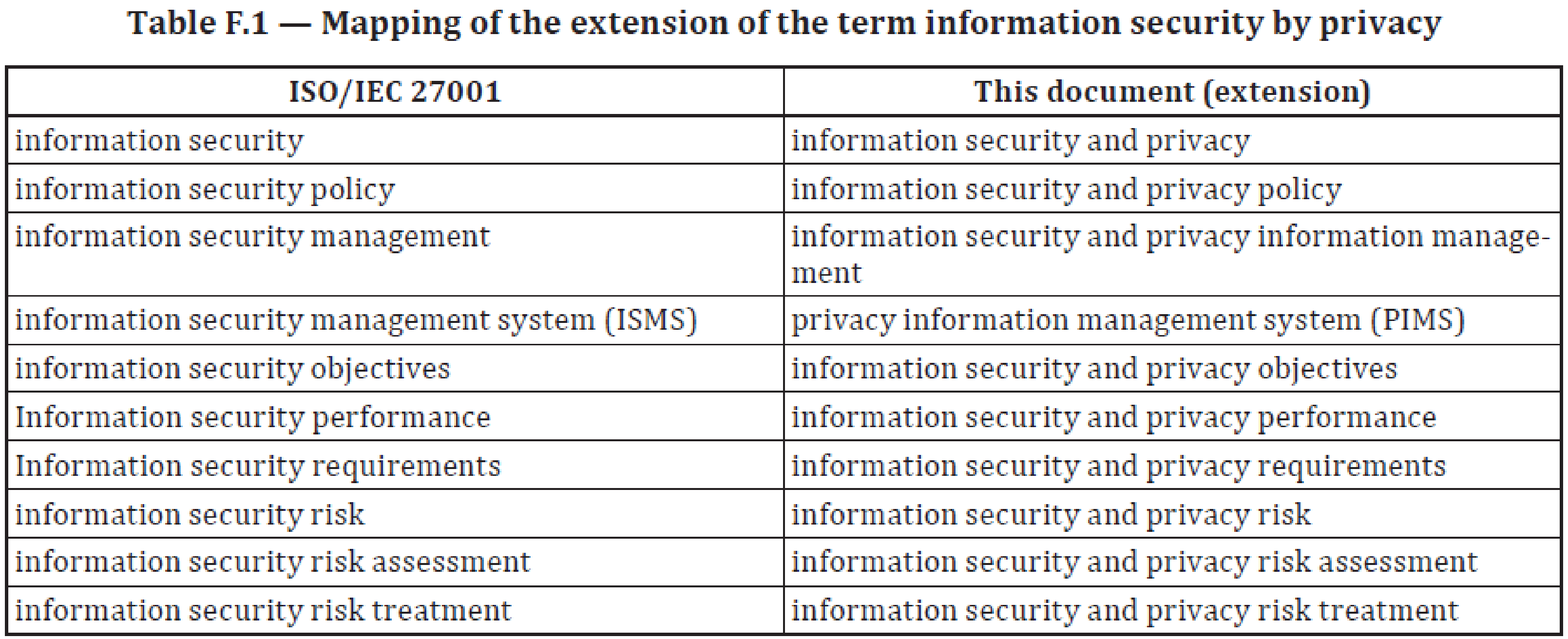
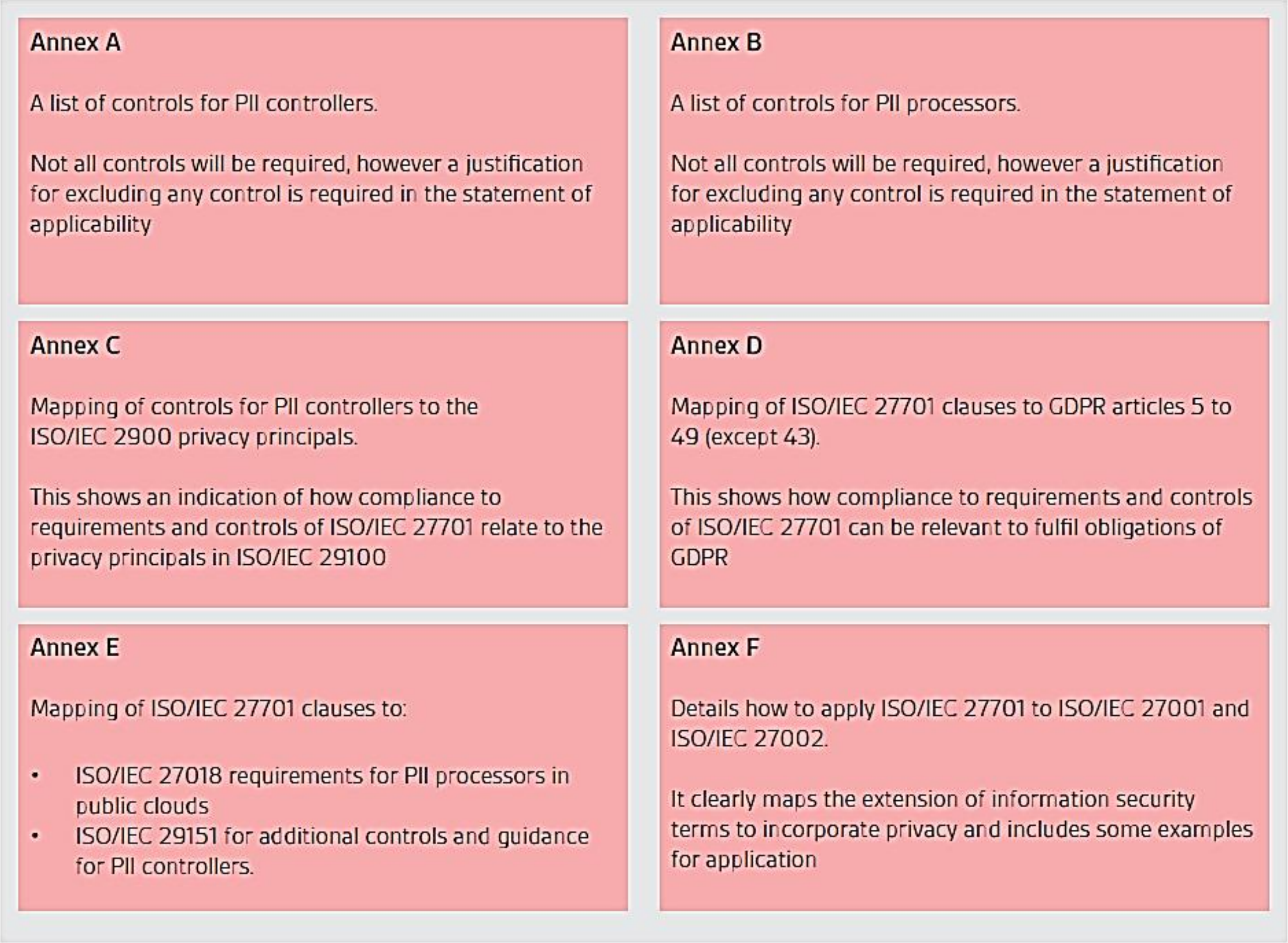


Table F.1 — Mapping of the extension of the term information security by privacy

ISO/IEC 27001	This document (extension)
information security	information security and privacy
information security policy	information security and privacy policy
information security management	information security and privacy information management
information security management system (ISMS)	privacy information management system (PIMS)
information security objectives	information security and privacy objectives
Information security performance	information security and privacy performance
Information security requirements	information security and privacy requirements
information security risk	information security and privacy risk
information security risk assessment	information security and privacy risk assessment
information security risk treatment	information security and privacy risk treatment

Sumber : SNI ISO/IEC 27701:2019

27701: 2019



Annex A

A list of controls for PII controllers.

Not all controls will be required, however a justification for excluding any control is required in the statement of applicability

Annex B

A list of controls for PII processors.

Not all controls will be required, however a justification for excluding any control is required in the statement of applicability

Annex C

Mapping of controls for PII controllers to the ISO/IEC 2900 privacy principals.

This shows an indication of how compliance to requirements and controls of ISO/IEC 27701 relate to the privacy principals in ISO/IEC 29100

Annex D

Mapping of ISO/IEC 27701 clauses to GDPR articles 5 to 49 (except 43).

This shows how compliance to requirements and controls of ISO/IEC 27701 can be relevant to fulfil obligations of GDPR

Annex E

Mapping of ISO/IEC 27701 clauses to:

- ISO/IEC 27018 requirements for PII processors in public clouds
- ISO/IEC 29151 for additional controls and guidance for PII controllers.

Annex F

Details how to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002.

It clearly maps the extension of information security terms to incorporate privacy and includes some examples for application

Sumber : ISO/IEC 27701 Privacy Information Management Your implementation guide - BSI

DIS 27701

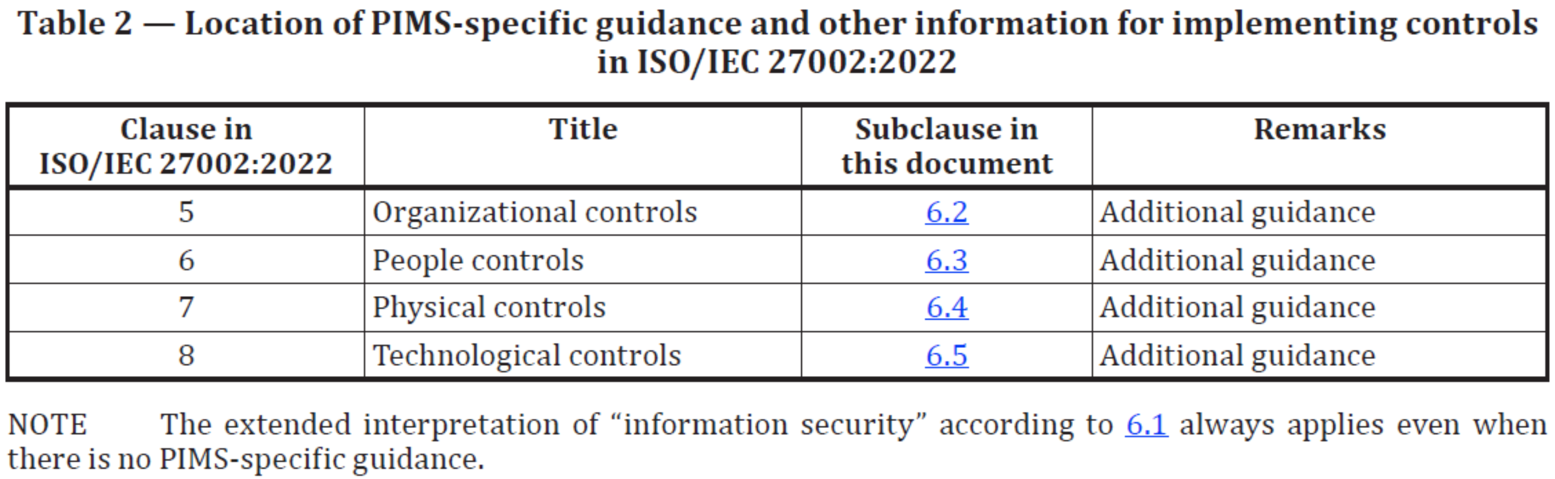


Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2022

Clause in ISO/IEC 27002:2022	Title	Subclause in this document	Remarks
5	Organizational controls	6.2	Additional guidance
6	People controls	6.3	Additional guidance
7	Physical controls	6.4	Additional guidance
8	Technological controls	6.5	Additional guidance

NOTE The extended interpretation of “information security” according to 6.1 always applies even when there is no PIMS-specific guidance.

Sumber : DIS ISO/IEC 27701

Diskusi

Terima Kasih Telah Berpartisipasi