Penerapan UU PDP Pada SMKI

Harun Al Rasyid
ISMSF.ID
27 Januari 2023

Harun Al Rasyid, SE, CISA, CDPSE, GRCP, GRCA, COBIT-F, CEHv11, CSX-F, ISMS27001LA, QMS9001IA

//inditech

- ❏ Founder & Partner Inditech sejak 2011
- ❏ IT Background selama 20+ tahun
- ❏ Anggota KomTek 35-01 BSN tentang Teknologi Informasi = mirror JTC 1
- ❏ Anggota WG2 SNI bidang Tata Kelola TI dan Manajemen Layanan
- ❏ Anggota WG8 SNI bidang Rekayasa Perangkat Lunak (RPL)
- ❏ Anggota Gugus Kerja 1 bidang SMKI
- ❏ Tim Perumus Peta Okupasi Kamsiber
- ❏ Tim Perumus SKKNI AKI

ISACA. Indonesia Chapter

- ❏ Vice President 2021 - 2023
- ❏ Chapter Secretary 2019 – 2021
- ❏ Chapter Secretary 2017 – 2019
- ❏ Government & Regulatory Advocate (GRA) 2015 – 2017
- ❏ Program Director 2014 – 2015
- ❏ Member since 15 March 2010

Gold LEVEL

Founder @ Inditech
PT Insan Dikara Technology

- CISA
- CDPSE
- GRCP
- GRCA
- COBIT5F & 2019F
- CEHv11
- CSX-F
- ISMS 27001-LA
- QMS 9001-IA

Tentang Perusahaan Kami

//inditech

OUR VISION
To be dependable provider of IT Governance, Risk, Compliance and Assurance advisory services.

ASSURANCE

- IT & Security Audit
- Capability & Maturity Assessment
- IT Due Dilligence
- IT Compliance

CONSULTING

- IT Governance
- IT & Security Planning
- ISMS Implementation
- IT Risk Management
- IT Service Management
- IT Business Continuity

TRAINING & DEVELOPMENT

- ISMS Awareness & Internal Audit
- IT Governance using COBIT Framework
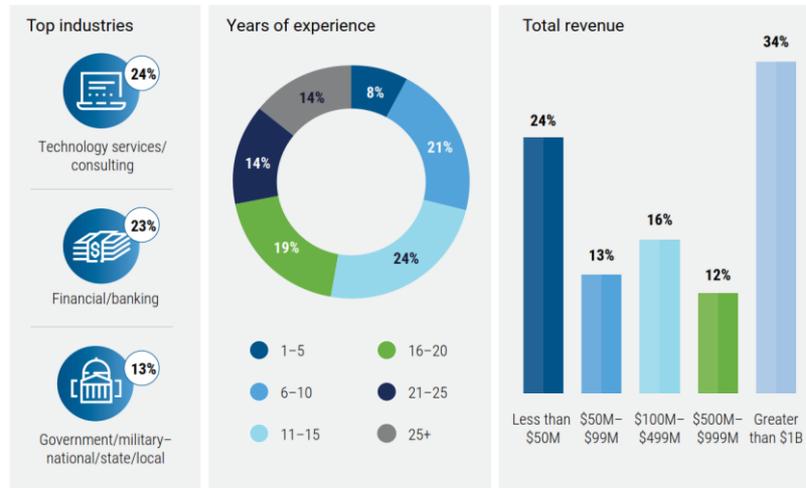- IT Infrastructure Library & Operation
- IT Risk Management
- CISA Exam Preparation

Privacy in Practice – ISACA 2023

Number of employees at organization

19%	16%	23%	18%	25%
1–249 employees	250–999 employees	1,000–4,999 employees	5,000–24,999 employees	25,000 or more employees

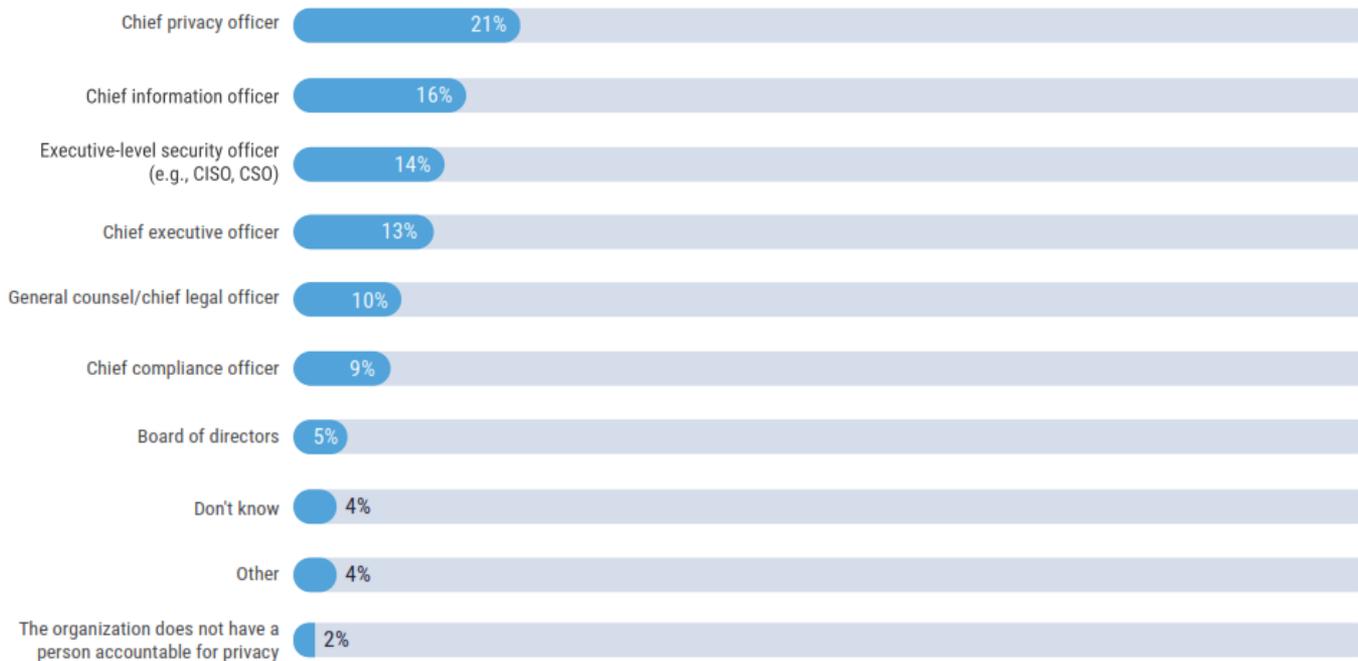### Privacy in Practice 2023

ISACA

Privacy

© 2023 ISACA. All Rights Reserved.

In the fourth quarter of 2022, ISACA sent survey invitations globally to 46,000 ISACA constituents who hold the ISACA CSX Cybersecurity Practitioner Certification™ (CSX-P™), Certified Information Security Manager® (CISM) or Certified Data Privacy Solutions Engineer™ (CDPSE™) designation, or have "privacy" in their job title

Top industries

- Technology services/consulting — 24%
- Financial/banking — 23%
- Government/military–national/state/local — 13%

Years of experience

- 1–5
- 6–10
- 11–15
- 16–20
- 21–25
- 25+

8%, 21%, 24%, 19%, 14%, 14%

Total revenue

Less than $50M	$50M–$99M	$100M–$499M	$500M–$999M	Greater than $1B
24%	13%	16%	12%	34%

Region

North America 47%
Latin America 4%
Africa 4%
Europe 20%
Middle East 4%
Asia 19%
Oceania 3%

Privacy in Practice – ISACA 2023
Akuntabilitas dalam pelindungan Data Privacy

FIGURE 8: Accountability for Privacy

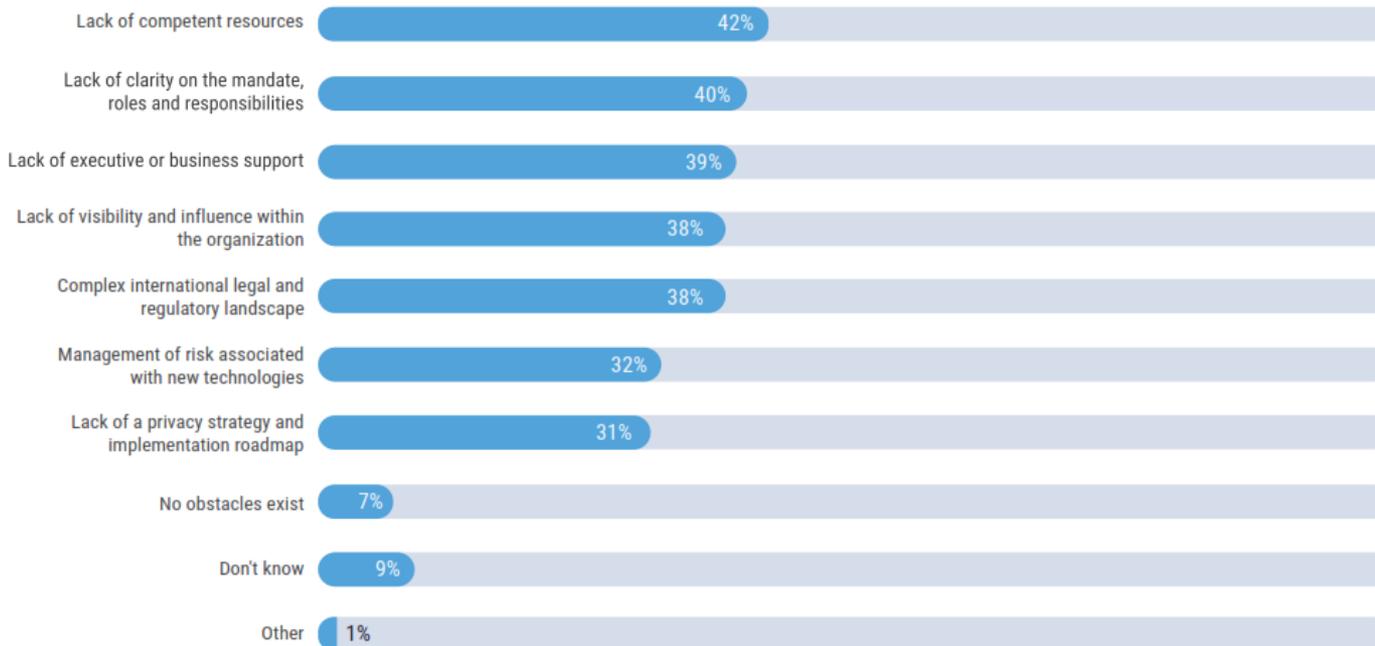Who is primarily accountable for privacy in your organization?

Chief privacy officer	21%
Chief information officer	16%
Executive-level security officer (e.g., CISO, CSO)	14%
Chief executive officer	13%
General counsel/chief legal officer	10%
Chief compliance officer	9%
Board of directors	5%
Don't know	4%
Other	4%
The organization does not have a person accountable for privacy	2%

Hambatan bagi Privacy Program

FIGURE 9: Obstacles to Forming a Privacy Program

Which, if any, of the following are obstacles faced by an organization in its ability to form a privacy program?

Select all that apply.

Obstacle	Percentage
Lack of competent resources	42%
Lack of clarity on the mandate, roles and responsibilities	40%
Lack of executive or business support	39%
Lack of visibility and influence within the organization	38%
Complex international legal and regulatory landscape	38%
Management of risk associated with new technologies	32%
Lack of a privacy strategy and implementation roadmap	31%
No obstacles exist	7%
Don't know	9%
Other	1%

Faktor-faktor Kegagalan Pelindungan Privasi

//inditech

FIGURE 15: Most Common Privacy Failures

In your opinion, which of the following are the most common privacy failures in an organization?

Select all that apply.

Category	Percentage
Lack of training or poor training	49%
Not practicing privacy by design	42%
Data breach/leakage	42%
Not performing a risk analysis	41%
Social engineering	39%
Bad or nonexistent detection of personal information	37%
Noncompliance with applicable laws and regulations	34%
Ethical decision making	16%
Don't know	10%
Other	2%
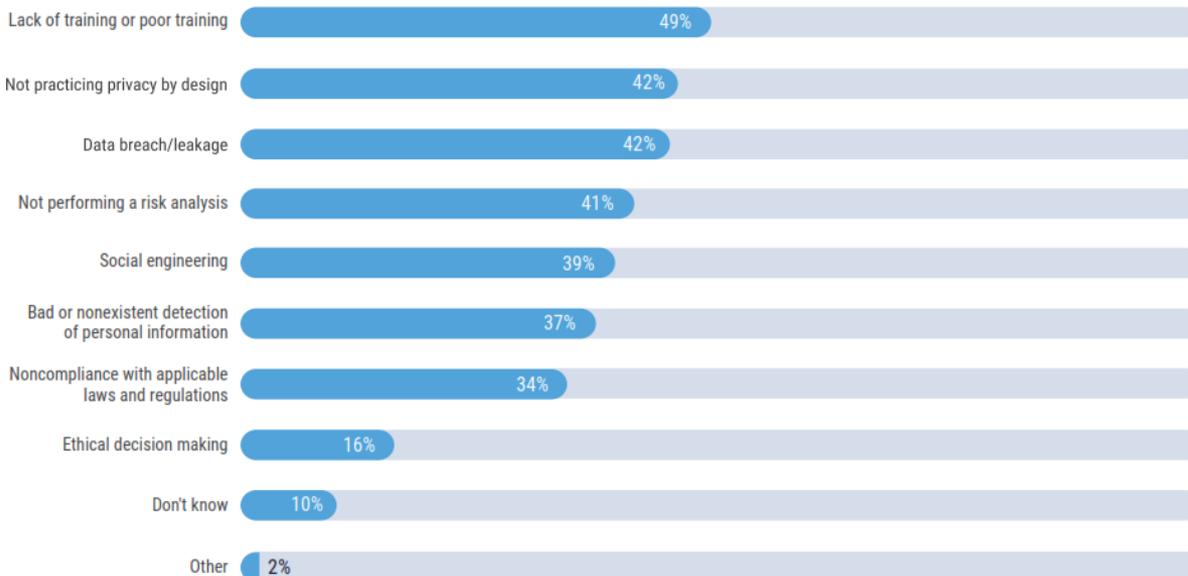
A challenge to quickly filling privacy roles is a lack of qualified applicants. Experience is the primary factor in determining an applicant's qualifications.

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi

❑ Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

❑ Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional Subjek Data Pribadi.

Konten UU PDP

//inditech
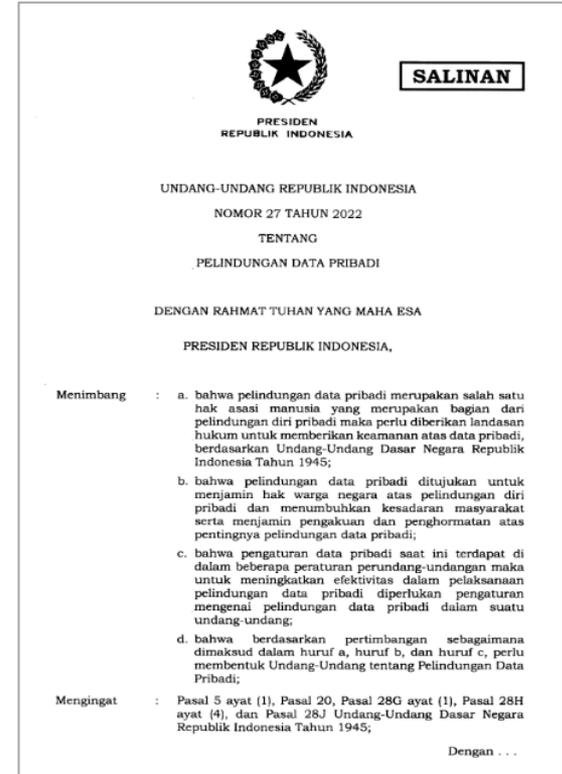
Ketentuan Umum (BAB I)

Definisi | Ruang lingkup

Kelembagaan (BAB IX)

Peran pemerintah dalam penyelenggaraan PDP, pelaksanaan penyelenggaraan PDP oleh Lembaga, tusi dan kewenangan lembaga

Asas (BAB II)

Asas Undang-Undang PDP

Jenis Data Pribadi (BAB III)

Data Pribadi Umum & Spesifik

Larangan dalam Penggunaan Data Pribadi (BAB XIII)

Setiap Orang dilarang dengan sengaja dan melawan hukum, mengumpulkan, mengungkapkan, menggunakan data pribadi yang bukan miliknya dan memalsukan Data Pribadi

Kerja Sama International (BAB X)

Kerja sama internasional dilakukan oleh Pemerintah dengan pemerintah negara lainatau organisasi inter7nsional terkait dengan PDP

Hak Subjek Data Pribadi (BAB IV)

Subjek Data Pribadi berhak untuk mendapatkan informasi, melengkapi, memperbarui, dan/atau memperbaiki kesalahan, hak akses, hak mengakhiri pemrosesan, hak menarik persetujuan, hak mengajukan keberatan, hak menunda/membatasi, hak menggugat dan menerima ganti rugi

Pemrosesan Data Pribadi (BAB V)

Lingkup pemrosesan

Prinsip pemrosesan

Ketentuan alat pemroses/pengolah data visual

Joint controller

Partisipasi Masyarakat (BAB XI)

Partisipasi dan peran masyarakat dalam mendukung terselenggaranya pelindungan data pribadi

Kewajiban Pengendali & Prosesor (BAB VI)

Lingkup pengendali & prosesor

Kewajiban Pengendali

Pengecualian terhadap Kewajiban Pengendali

Kewajiban Prosesor

Kewajiban penunjukkan DPO

Sanksi Administratif (BAB VIII)

Pengendali & Prosesor yang melakukan pelanggaran terhadap kewajiban dikenakan sanksi administrative (P57)

Pasal kewajiban : Pasal 20 ayat (1), Pasal 21 ayat (1) dan ayat (2), Pasal 24, Pasal 25 ayat (2), Pasal 26 ayat (3), Pasal 27, Pasal 28, Pasal 29, Pasal 30, Pasal 31, Pasal 32 ayat (1), Pasal 33, Pasal 34 ayat (1), Pasal 35, Pasal 36, Pasal 37, Pasal 38, asal 39 ayat (1), Pasal 40 ayat (1), Pasal 41 ayat (1) dan ayat (3), Pasal 42 ayat (1), Pasal 43 ayat (1), Pasal 44 ayat (1), Pasal 45, Pasal 46 ayat (1) dan ayat (3), Pasal 47, Pasal 48 ayat (1), Pasal 49, Pasal 51 ayat (1) dan ayat (5), Pasal 52, Pasal 53 ayat (1), Pasal 55 ayat (2), dan Pasal 56 ayat (2) sampai dengan ayat (4)

Sanksi administratif berupa: Peringatan tertulis, penghentian sementara kegiatan pemrosesan Data Pribadi, penghapusan atau pemusnahan Data Pribadi dan/atau denda administrative.

Ketentuan Pidana (BAB XIV)

Setiap Orang yang melakukan perbuatan yang dilaran sebagaimana dimaksud pada Pasal 65-66 akan dikenai sanksi pidana.

Pidana Korporasi

Pidana Tambahan

Penyelesaian Sengketa & Hukum Acara (BAB XII)

Melalui arbitrase, pengadilan atau Lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan. Alat bukti yang sah dalam UU PDP dan Proses persidangan

Transfer Data Pribadi (BAB VII)

Dalam wilayah RI

Luar wilayah RI

Ketentuan Peralihan (BAB XV)

UU PDP berlaku sejak diundangkan dan masa penyesuaian paling lama 2 tahun

Ketentuan Penutup (BAB XVI)

Dampak bagi Institusi

Governance

Privacy Strategy	Privacy Governance	DPO office	Establish Privacy Policies	Building Privacy Culture

Management

Privacy Protection	Data Management	DPIA	Data Subject Rights	Data Retention	Third party privacy risk
Concent Management	Data Processor Accountability	Cross Border Data Transfer	Record Of Processing Activities	Incident Management	Training & Awareness

Menjawab Kewajiban UU PDP dengan COBIT

COBIT® 2019 FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES

A.1.2 Mapping Table: Alignment Goals—Governance and Management Objectives

COBIT 2019 Alignment Goal to Privacy

AG07: Security of information, processing infrastructure and applications, and *privacy*

EDM03	Ensured risk optimization
APO12	Managed Risk
APO13	Managed Security
BAI10	Managed Configuration
DSS04	Managed Continuity
DSS05	Managed Security Services

COBIT® 2019 FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES

A.1.2 Mapping Table: Alignment Goals—Governance and Management Objectives
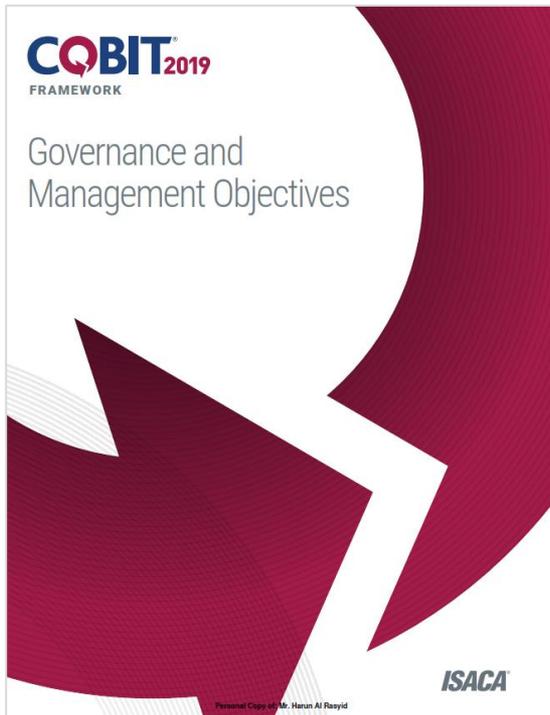
Figure—A.2 Mapping Governance and Management Objectives to Alignment Goals

298

Personal Copy of: Mr. Harun Al Rasyid

Implementasi PDP dengan COBIT 2019: Starting Point

APO13	Managed Security

APO 13.01	Establish and maintain an *information security management system* (ISMS)

APO 13.02	Define and manage an information security and privacy *risk treatment plan*.

APO 13.03	*Monitor and review* the information security management system (ISMS).

inditech

inditech

PT. INSAN DIKARA TECHNOLOGY

info@inditech.co.id

www.inditech.co.id

Governace
Risk
Compliance
Assurance

Legal Office:
Menara 165 Lt.4
Jl. TB. Simatupang Kav 1
Cilandak Timur, Pasar Minggu
Jakarta Selatan 12560

Basecamp:
Ruko Beverly
Jl. Pangeran Antasari No.67 i
Cilandak Barat, Kec. Cilandak
Jakarta Selatan 12430