

Sistem Manajemen Kecerdasan Buatan (AIMS)

Pemahaman dan Penerapan **ISO/IEC 42001:2023**
dalam Keamanan Informasi, Keamanan Siber, dan
Perlindungan Data Pribadi

AI GOVERNANCE
RISK MANAGEMENT
TRUSTED AI
COMPLIANCE
SUSTAINABLE FUTURE



KEAMANAN
INFORMASI



KEAMANAN
SIBER



PERLINDUNGAN
DATA PRIBADI

DATA
PEOPLE
TRUST
A BETTER
HUMAN FUTURE

PEOPLE | PROCESS | TECHNOLOGY | GOVERNANCE

Penulis:

Dr. Nungky Awang Chandra, S.Si., M.TI.
Siti Maesaroh, S.Kom., M.T.I.

Mohamad Yusuf, S.Kom., M.C.S.
Diva Alifta Chandra, B.Eng., M.Sc.

SISTEM MANAJEMEN KECERDASAN BUATAN (AIMS)

Pemahaman dan Penerapan ISO/IEC 42001:2023
dalam Keamanan Informasi, Keamanan Siber, dan
Perlindungan Data Pribadi

Dr. Nungky Awang Chandra, S.Si., M.TI.

Siti Maesaroh, S.Kom., M.T.I.

Mohamad Yusuf, S.Kom., M.C.S.

Diva Alifta Chandra, B.Eng., M.Sc.

SISTEM MANAJEMEN KECERDASAN BUATAN (AIMS)

Pemahaman dan Penerapan ISO/IEC 42001:2023 dalam Keamanan
Informasi, Keamanan Siber, dan Perlindungan Data Pribadi

Penulis:

Dr. Nungky Awang Chandra, S.Si., M.TI.

Siti Maesaroh, S.Kom., M.T.I.

Mohamad Yusuf, S.Kom., M.C.S.

Diva Alifta Chandra, B.Eng., M.Sc.

Tata Letak : Lilis Khalisatul Karimah
Desain Cover : Lilis Khalisatul Karimah
Ukuran : UNESCO 15,5 x 23 cm
Halaman : xvii, 175
ISBN : 978-634-7949-05-9
Terbit Pada : September 2026
Anggota IKAPI : No. 073/BANTEN/2023

Hak Cipta 2026 @ Sada Kurnia Pustaka dan Penulis

Hak cipta dilindungi undang-undang dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara apapun tanpa izin tertulis dari penerbit dan penulis.

PENERBIT PT SADA KURNIA PUSTAKA

Jl. Kramat, Panenjoan Kec. Carenang, Kab. Serang – Banten, 42195

Email : sadapenerbit@gmail.com

Website : sadapenerbit.com & repository.sadapenerbit.com

Telpon/WA : +62 838 1281 8431

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga buku Sistem Manajemen Kecerdasan Buatan (AIMS): Pemahaman dan Penerapan ISO/IEC 42001:2023 dalam Keamanan Informasi, Keamanan Siber, dan Perlindungan Data Pribadi dapat diselesaikan dengan baik.

Kecerdasan buatan telah berkembang menjadi teknologi yang memengaruhi hampir seluruh aspek kehidupan dan kegiatan organisasi. Kehadiran *Generative AI*, *Large Language Model*, dan *AI agent* membuka peluang peningkatan produktivitas yang sangat besar, tetapi juga menghadirkan risiko baru, mulai dari kebocoran data, serangan terhadap model, keputusan yang tidak adil, hingga dampak sosial yang lebih luas. Di tengah perubahan yang cepat tersebut, organisasi membutuhkan kerangka tata kelola yang tidak hanya berisi prinsip, tetapi juga dapat diterapkan, diukur, dan diaudit.

ISO/IEC 42001:2023 hadir sebagai standar sistem manajemen kecerdasan buatan pertama yang dapat disertifikasi. Standar ini melengkapi standar yang telah lebih dahulu dikenal luas di Indonesia, seperti ISO/IEC 27001 untuk keamanan informasi dan ISO/IEC 27701 untuk manajemen informasi privasi. Bersama dengan berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan pedoman etika kecerdasan artifisial nasional, kebutuhan akan pemahaman yang utuh tentang tata kelola AI menjadi semakin mendesak.

Buku ini disusun untuk menjawab kebutuhan tersebut dengan menyajikan pembahasan yang sistematis, mulai dari konsep dasar AI, struktur dan persyaratan ISO/IEC 42001, manajemen risiko dan penilaian dampak, kontrol Annex A, keamanan sistem AI, integrasi dengan keamanan informasi dan perlindungan data pribadi, keamanan *Generative AI*, hingga implementasi, audit, sertifikasi, dan studi kasus.

Setiap bab dilengkapi tabel, gambar, contoh penerapan, serta *checklist* evaluasi agar mudah digunakan sebagai rujukan kerja.

Kami menyampaikan terima kasih kepada semua pihak yang telah memberikan dukungan, masukan, dan inspirasi dalam penyusunan buku ini, termasuk rekan akademisi di Universitas Mercu Buana, para praktisi keamanan informasi dan auditor sistem manajemen, serta Penerbit Sada Kurnia Pustaka. Kami menyadari bahwa buku ini masih memiliki keterbatasan, sehingga kritik dan saran yang membangun sangat kami harapkan untuk penyempurnaan edisi berikutnya. Semoga buku ini bermanfaat bagi pembaca dalam membangun AI yang aman, bertanggung jawab, dan terpercaya.

Penulis

PRAKATA

Buku ini ditujukan bagi praktisi kecerdasan buatan, *AI governance officer*, praktisi keamanan informasi dan keamanan siber, *data protection officer*, auditor ISO/IEC 42001 dan ISO/IEC 27001, konsultan sistem manajemen, manajer TI, CIO dan CISO, pengembang AI, *data scientist*, manajer risiko, *compliance officer*, akademisi, serta mahasiswa yang ingin memahami tata kelola AI secara praktis.

Pendekatan yang digunakan dalam buku ini adalah pendekatan berbasis risiko, berbasis siklus hidup, berbasis kontrol, *security by design*, *privacy by design*, dan *responsible AI*. ISO/IEC 42001:2023 dijadikan kerangka utama, kemudian diperkaya dengan panduan dari ISO/IEC 22989 tentang konsep dan terminologi AI, ISO/IEC 23894 tentang manajemen risiko AI, dan ISO/IEC 42005 tentang penilaian dampak sistem AI, serta dikaitkan dengan ISO/IEC 27001, ISO/IEC 27701, dan ketentuan perlindungan data pribadi di Indonesia.

Buku ini terdiri atas lima belas bab. Bab 1 sampai Bab 3 membahas fondasi AI, pemahaman ISO/IEC 42001, serta konteks organisasi dan tata kelola AI. Bab 4 sampai Bab 7 membahas perencanaan dan manajemen risiko, dukungan dan operasional, siklus hidup sistem AI dan tata kelola data, serta kontrol Annex A. Bab 8 sampai Bab 10 membahas penilaian dampak dan *responsible AI*, AI dalam keamanan informasi dan siber, serta integrasi AIMS dengan keamanan informasi dan perlindungan data pribadi. Bab 11 membahas keamanan *Generative AI*, LLM, RAG, dan *AI agent*. Bab 12 sampai Bab 14 membahas implementasi, audit dan sertifikasi, serta studi kasus. Bab 15 menyajikan kesimpulan, model kematangan, dan rekomendasi. Lampiran berisi template yang dapat langsung disesuaikan, seperti inventaris sistem AI, *risk register*, penilaian dampak, kebijakan AI, matriks kontrol, dan *checklist* audit.

Uraian klausul dan kontrol standar dalam buku ini merupakan interpretasi dan terjemahan penulis untuk tujuan pembelajaran.

Untuk keperluan kepatuhan dan sertifikasi, pembaca dianjurkan merujuk teks resmi standar yang diterbitkan ISO dan IEC. Studi kasus yang disajikan bersifat ilustratif dan tidak merujuk pada organisasi tertentu.

Penulis berharap buku ini dapat menjadi pendamping praktis bagi organisasi dalam perjalanan membangun, menerapkan, memelihara, dan meningkatkan sistem manajemen kecerdasan buatan, sekaligus menjadi bahan ajar yang relevan bagi dunia pendidikan tinggi di Indonesia.

Jakarta, September 2026

Penulis

DAFTAR ISI

KATA PENGANTAR	iii
PRAKATA.....	v
DAFTAR ISI	vii
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xvii
BAB 1 PENDAHULUAN KECERDASAN BUATAN DAN AIMS	1
A. Perkembangan <i>Artificial Intelligence</i>	1
B. <i>Machine Learning</i> , <i>Deep Learning</i> , dan <i>Generative AI</i>	2
C. <i>Large Language Model</i> , <i>AI Agent</i> , dan <i>Agentic AI</i>	4
D. Pemanfaatan AI dalam Organisasi.....	5
E. Risiko dan Dampak <i>Artificial intelligence</i>	6
F. <i>AI Governance</i> dan <i>Responsible AI</i>	7
G. <i>Artificial Intelligence Management System</i>	8
H. Tujuan dan Struktur Buku.....	9
I. Ringkasan dan <i>Checklist</i> Evaluasi	10
BAB 2 MEMAHAMI ISO/IEC 42001:2023	11
A. Latar Belakang ISO/IEC 42001	11
B. Tujuan dan Manfaat AIMS	12
C. Struktur ISO/IEC 42001:2023.....	13
D. Prinsip Sistem Manajemen AI.....	15
E. Peran <i>AI Provider</i> , <i>Developer</i> , <i>Producer</i> , dan <i>User</i>	16
F. <i>Responsible Development</i> dan <i>Responsible Use</i>	17
G. Hubungan ISO/IEC 42001 dengan Sistem Manajemen Lain	18
H. Sertifikasi ISO/IEC 42001.....	20
I. Ringkasan dan <i>Checklist</i> Evaluasi	20
BAB 3 KONTEKS ORGANISASI DAN TATA KELOLA AI	22
A. Konteks Internal dan Eksternal	22
B. <i>Interested Parties</i>	23
C. Penetapan Ruang Lingkup AIMS	24
D. <i>Leadership</i> dan <i>Commitment</i>	25
E. <i>Artificial Intelligence Policy</i>	26
F. Struktur <i>AI Governance</i>	27

G.	<i>AI Governance Committee</i>	28
H.	<i>Roles, Responsibilities, dan Authorities</i>	28
I.	<i>Accountability dan Human Oversight</i>	29
J.	Ringkasan dan <i>Checklist</i> Evaluasi	30
BAB 4 PERENCANAAN DAN MANAJEMEN RISIKO AI		31
A.	Risiko dan Peluang <i>Artificial Intelligence</i>	31
B.	Identifikasi Risiko AI	32
C.	<i>AI Risk Assessment</i>	33
D.	<i>Likelihood, Impact, dan Risk Level</i>	34
E.	<i>AI Risk Treatment</i>	36
F.	<i>Residual Risk</i>	37
G.	Sasaran AIMS dan KPI/KRI	38
H.	<i>AI Risk Register</i>	39
I.	Integrasi dengan <i>Enterprise Risk Management</i>	40
J.	Perencanaan Perubahan	40
K.	Ringkasan dan <i>Checklist</i> Evaluasi	41
BAB 5 DUKUNGAN DAN OPERASIONAL SISTEM AI		42
A.	<i>Resources</i>	42
B.	Kompetensi Personel.....	43
C.	<i>Awareness dan Training</i>	44
D.	<i>Communication</i>	44
E.	<i>Documented Information</i>	45
F.	<i>Operational Planning and Control</i>	46
G.	Pengadaan dan Pengembangan AI	46
H.	<i>Third-party AI</i>	47
I.	<i>Human Oversight</i>	48
J.	Pengendalian Perubahan Sistem AI	49
K.	Ringkasan dan <i>Checklist</i> Evaluasi	49
BAB 6 SIKLUS HIDUP SISTEM AI DAN DATA GOVERNANCE		51
A.	<i>AI System Lifecycle</i>	51
B.	<i>Concept dan Design</i>	52
C.	<i>Data Collection dan Acquisition</i>	53
D.	<i>Data Labelling dan Preparation</i>	54
E.	<i>Training, Validation, dan Testing Dataset</i>	54
F.	<i>Development dan Training Model</i>	55
G.	<i>Validation dan Testing Model</i>	56

H.	<i>Deployment dan Operation</i>	56
I.	<i>Monitoring Model, Model Drift, dan Data Drift</i>	57
J.	<i>Retirement dan Decommissioning</i>	59
K.	<i>Data Quality dan Data Lineage</i>	59
L.	<i>Ringkasan dan Checklist Evaluasi</i>	60
BAB 7 ANNEX A CONTROLS ISO/IEC 42001		61
A.	<i>Konsep Pengendalian AIMS</i>	61
B.	<i>Policies Related to AI dan Internal Organization</i>	62
C.	<i>Resources for AI Systems</i>	62
D.	<i>Assessing Impacts of AI Systems</i>	63
E.	<i>AI System Lifecycle Controls</i>	64
F.	<i>Data for AI Systems</i>	64
G.	<i>Information for Interested Parties</i>	65
H.	<i>Use of AI Systems</i>	66
I.	<i>Third-party and Customer Relationships</i>	66
J.	<i>Pemilihan Controls Berdasarkan Risiko</i>	67
K.	<i>Control Effectiveness dan Evidence</i>	68
L.	<i>AIMS Control Matrix</i>	69
M.	<i>Ringkasan dan Checklist Evaluasi</i>	69
BAB 8 AI SYSTEM IMPACT ASSESSMENT, ETIKA, DAN RESPONSIBLE AI		71
A.	<i>Konsep AI System Impact Assessment</i>	71
B.	<i>Dampak terhadap Individu</i>	73
C.	<i>Dampak terhadap Kelompok dan Masyarakat</i>	74
D.	<i>Bias dan Discrimination</i>	74
E.	<i>Hallucination</i>	75
F.	<i>Automation Bias</i>	76
G.	<i>Fairness</i>	76
H.	<i>Transparency dan Explainability</i>	77
I.	<i>Accountability dan Human Oversight</i>	78
J.	<i>Ethical AI dan Responsible AI</i>	78
K.	<i>Ringkasan dan Checklist Evaluasi</i>	79
BAB 9 AI DALAM KEAMANAN INFORMASI DAN KEAMANAN SIBER		81
A.	<i>AI dan Confidentiality, Integrity, Availability</i>	81
B.	<i>Threat dan Vulnerability pada Sistem AI</i>	82

C.	<i>Prompt Injection dan Jailbreaking</i>	83
D.	<i>Sensitive Information Disclosure</i>	84
E.	<i>Data dan Model Poisoning</i>	84
F.	<i>Model Extraction dan Adversarial Machine Learning</i>	85
G.	<i>AI Supply-chain Risk</i>	86
H.	<i>Shadow AI</i>	86
I.	<i>AI untuk Threat Detection dan Security Operations Center</i>	87
J.	<i>AI untuk Malware, Ransomware, dan Phishing Detection</i>	88
K.	<i>AI untuk Vulnerability Management</i>	88
L.	<i>Ringkasan dan Checklist Evaluasi</i>	89
BAB 10 AIMS, KEAMANAN INFORMASI, DAN PERLINDUNGAN		
DATA PRIBADI		90
A.	<i>Integrasi AIMS dan ISMS</i>	90
B.	<i>Hubungan ISO/IEC 42001 dan ISO/IEC 27001</i>	91
C.	<i>Integrated Risk Assessment</i>	93
D.	<i>Identity and Access Management serta Logging and Monitoring</i>	94
E.	<i>Secure AI Development dan Supplier Security</i>	94
F.	<i>AI Incident Management</i>	95
G.	<i>Personal Data dalam Sistem AI</i>	95
H.	<i>Privacy by Design, Data Minimization, dan Anonymization</i>	96
I.	<i>Privacy Impact Assessment</i>	97
J.	<i>Perlindungan Data Pribadi Indonesia</i>	98
K.	<i>Integrasi AIMS–ISMS–Privacy</i>	99
L.	<i>Ringkasan dan Checklist Evaluasi</i>	99
BAB 11 KEAMANAN GENERATIVE AI, LLM, RAG, DAN AI		
AGENT		101
A.	<i>Generative AI dan Large Language Model</i>	101
B.	<i>Prompt dan Prompt Security</i>	102
C.	<i>Risiko Kebocoran Data dan Penggunaan AI Publik</i>	103
D.	<i>Retrieval-Augmented Generation</i>	104
E.	<i>Vector Database Security</i>	104
F.	<i>AI Agent dan Agentic AI</i>	105
G.	<i>Risiko Autonomous AI Agent</i>	105
H.	<i>API Security</i>	106
I.	<i>Secure AI Gateway</i>	107

J.	<i>Monitoring dan Logging AI</i>	107
K.	<i>Secure Generative AI Architecture</i>	107
L.	Ringkasan dan <i>Checklist</i> Evaluasi	108
BAB 12 IMPLEMENTASI AIMS		110
A.	<i>Gap Analysis</i> ISO/IEC 42001	110
B.	Penetapan <i>Scope</i>	111
C.	<i>AI System Inventory</i>	112
D.	Penyusunan <i>AI Policy</i> dan Dokumen AIMS	113
E.	<i>AI Risk Assessment</i> dan <i>AI Impact Assessment</i>	113
F.	Penetapan <i>Controls</i> dan SoA.....	114
G.	<i>Training</i> dan <i>Awareness</i>	114
H.	Tahapan Implementasi	115
I.	<i>Roadmap</i> Implementasi AIMS 30–60–90 Hari	115
J.	Faktor Keberhasilan dan Tantangan	116
K.	Ringkasan dan <i>Checklist</i> Evaluasi	117
BAB 13 AUDIT DAN SERTIFIKASI AIMS		118
A.	Pemantauan, Pengukuran, Analisis, dan Evaluasi	118
B.	Internal Audit AIMS	119
C.	<i>Management Review</i>	120
D.	<i>Nonconformity</i> dan <i>Corrective Action</i>	121
E.	<i>Continual Improvement</i>	121
F.	Audit Stage 1 dan Stage 2.....	122
G.	<i>Surveillance Audit</i> dan Resertifikasi.....	123
H.	Ringkasan dan <i>Checklist</i> Evaluasi	123
BAB 14 STUDI KASUS PENERAPAN AIMS		125
A.	AI untuk <i>Security Operations Center</i>	125
B.	AI untuk Deteksi <i>Intrusion</i> dan <i>Cyberattack</i>	126
C.	AI untuk <i>Phishing</i> dan <i>Malware Detection</i>	126
D.	AI untuk <i>Penetration Testing</i>	127
E.	Kebocoran Data melalui <i>Generative AI</i>	127
F.	<i>Prompt Injection</i> pada <i>Corporate AI Chatbot</i>	128
G.	<i>Shadow AI</i> dalam Organisasi	128
H.	AI untuk <i>Data Loss Prevention</i>	129
I.	AI dalam Perlindungan Data Pribadi.....	130
J.	<i>Facial Recognition</i> dan <i>Biometric AI</i>	130
K.	AI pada Perbankan dan <i>Fintech</i>	131

L. AI pada <i>Healthcare</i>	131
M. Ringkasan dan Pelajaran Studi Kasus.....	132
BAB 15 KESIMPULAN, MODEL KEMATANGAN, DAN	
REKOMENDASI	134
A. Kesimpulan.....	134
B. Model Kematangan AIMS.....	135
C. Rekomendasi bagi Organisasi.....	136
D. Rekomendasi bagi Regulator, Akademisi, dan Profesi	136
E. Arah Pengembangan AIMS ke Depan.....	137
F. Penutup	137
LAMPIRAN.....	139
DAFTAR SINGKATAN	155
DAFTAR PUSTAKA.....	158
GLOSARIUM	164
INDEKS	170
BIOGRAFI PENULIS.....	173

DAFTAR TABEL

Tabel 1. 1: Jenis Pendekatan *Machine Learning*3

Tabel 1. 2: Perbandingan *Chatbot* LLM, Aplikasi RAG, dan *AI Agent*5

Tabel 1. 3: Contoh Pemanfaatan AI Lintas Sektor6

Tabel 1. 4: Prinsip *Responsible* AI dari Beberapa Kerangka Rujukan ...8

Tabel 1. 5: Struktur Isi Buku9

Tabel 1. 6: *Checklist* Evaluasi Bab 110

Tabel 2. 1: Manfaat Penerapan AIMS bagi Organisasi.....12

Tabel 2. 2: Struktur Klausul ISO/IEC 42001:202313

Tabel 2. 3: Lampiran ISO/IEC 42001:202314

Tabel 2. 4: Istilah Kunci dalam Penerapan AIMS15

Tabel 2. 5: Prinsip Sistem Manajemen dan Penerapannya pada AI....16

Tabel 2. 6: Peran Pemangku Kepentingan AI Menurut ISO/IEC
2298916

Tabel 2. 7: Perbandingan *Responsible Development* dan *Responsible
Use*.....18

Tabel 2. 8: Integrasi AIMS dengan Standar Sistem Manajemen Lain.19

Tabel 2. 9: *Checklist* Evaluasi Bab 2.....20

Tabel 3. 1: Contoh Isu Konteks untuk AIMS23

Tabel 3. 2: Contoh Pihak Berkepentingan dan Kebutuhannya24

Tabel 3. 3: Bentuk Komitmen Manajemen Puncak dan Buktinya.....25

Tabel 3. 4: Kerangka Isi Kebijakan AI.....26

Tabel 3. 5: Contoh Piagam Komite Tata Kelola AI.....28

Tabel 3. 6: Contoh Matriks RACI Aktivitas AIMS.....29

Tabel 3. 7: *Checklist* Evaluasi Bab 3.....30

Tabel 4. 1: Katalog Sumber Risiko AI32

Tabel 4. 2: Skala Kemungkinan Risiko AI34

Tabel 4. 3: Skala Dampak Risiko AI Tiga Dimensi35

Tabel 4. 4: Kriteria Tingkat Risiko dan Keputusan36

Tabel 4. 5: Opsi Perlakuan Risiko AI37

Tabel 4. 6: Contoh Perhitungan Risiko Residual.....38

Tabel 4. 7: Contoh Sasaran AI dengan KPI dan KRI38

Tabel 4. 8: Contoh Ringkas AI Risk Register39

Tabel 4. 9: Contoh Pemicu Perubahan dan Tindakan Perencanaan...	40
Tabel 4. 10: Checklist Evaluasi Bab 4	41
Tabel 5. 1: Jenis Sumber Daya Sistem AI Menurut Kontrol A.4	42
Tabel 5. 2: Contoh Matriks Kompetensi AIMS.....	43
Tabel 5. 3: Contoh Program <i>Awareness</i> dan Pelatihan AI	44
Tabel 5. 4: Contoh Rencana Komunikasi AIMS	44
Tabel 5. 5: Informasi Terdokumentasi Minimum AIMS	45
Tabel 5. 6: Perbandingan Jalur Perolehan AI	46
Tabel 5. 7: Klausul Kontrak Penting untuk Layanan AI Pihak Ketiga	47
Tabel 5. 8: Kategori Perubahan Sistem AI dan Pengendaliannya.....	49
Tabel 5. 9: <i>Checklist</i> Evaluasi Bab 5	50
Tabel 6. 1: Pemetaan Tahap Siklus Hidup dan Kontrol ISO/IEC 42001	52
Tabel 6. 2: Contoh Persyaratan Sistem AI pada Tahap Desain	53
Tabel 6. 3: Kriteria Penilaian Sumber Data	54
Tabel 6. 4: Pembagian dan Pengendalian Dataset.....	55
Tabel 6. 5: Dimensi Pengujian Sistem AI	56
Tabel 6. 6: Contoh Isi Log Kejadian Sistem AI	57
Tabel 6. 7: Indikator Pemantauan Model dan Tindakan.....	58
Tabel 6. 8: Dimensi Kualitas Data untuk Sistem AI.....	59
Tabel 6. 9: <i>Checklist</i> Evaluasi Bab 6.....	60
Tabel 7. 1: Kontrol A.2 dan A.3	62
Tabel 7. 2: Kontrol A.4	63
Tabel 7. 3: Kontrol A.5	63
Tabel 7. 4: Kontrol A.6	64
Tabel 7. 5: Kontrol A.7	65
Tabel 7. 6: Kontrol A.8	65
Tabel 7. 7: Kontrol A.9	66
Tabel 7. 8: Kontrol A.10.....	66
Tabel 7. 9: Contoh Potongan Statement of Applicability	67
Tabel 7. 10: Jenis Bukti Efektivitas Kontrol.....	68
Tabel 7. 11: Contoh AIMS Control Matrix.....	69
Tabel 7. 12: <i>Checklist</i> Evaluasi Bab 7	70
Tabel 8. 1: Perbandingan AIIA, Penilaian Risiko AI, dan DPIA.....	72
Tabel 8. 2: Komponen Dokumentasi AIIA	73

Tabel 8. 3: Contoh Dampak Sistem AI terhadap Individu.....74

Tabel 8. 4: Sumber Bias dalam Sistem AI75

Tabel 8. 5: Metrik Keadilan yang Umum Digunakan.....76

Tabel 8. 6: Tingkat Transparansi Menurut Pemangku Kepentingan .77

Tabel 8. 7: Pemetaan Prinsip Responsible AI ke AIMS79

Tabel 8. 8: *Checklist* Evaluasi Bab 8.....79

Tabel 9. 1: Penerapan Prinsip CIA pada Sistem AI81

Tabel 9. 2: OWASP Top 10 for LLM *Applications* 202583

Tabel 9. 3: Serangan Adversarial dan Pengendaliannya.....85

Tabel 9. 4: Pemanfaatan AI untuk Deteksi Ancaman88

Tabel 9. 5: *Checklist* Evaluasi Bab 9.....89

Tabel 10. 1: Perbandingan Klausul ISO/IEC 42001 dan ISO/IEC
2700191

Tabel 10. 2: Pemetaan Kontrol ISO/IEC 27002 untuk Keamanan
Sistem AI.....92

Tabel 10. 3: Contoh Penilaian Risiko Terintegrasi.....93

Tabel 10. 4: Kategori Insiden AI dan Contoh Respons95

Tabel 10. 5: *Privacy-Enhancing Technologies* untuk AI.....97

Tabel 10. 6: Ketentuan UU PDP yang Relevan bagi Sistem AI98

Tabel 10. 7: Elemen Integrasi AIMS, ISMS, dan PIMS99

Tabel 10. 8: Checklist Evaluasi Bab 10 100

Tabel 11. 1: Pola Pemanfaatan Generative AI di Organisasi 101

Tabel 11. 2: Praktik Keamanan *Prompt*..... 102

Tabel 11. 3: Matriks Penggunaan AI Berdasarkan Klasifikasi Data. 103

Tabel 11. 4: Kontrol Keamanan Basis Data Vektor 104

Tabel 11. 5: Risiko AI Agent dan Pengendaliannya 106

Tabel 11. 6: Fungsi Utama AI Gateway 107

Tabel 11. 7: Checklist Evaluasi Bab 11 108

Tabel 12. 1: Skala Penilaian Tingkat Pemenuhan..... 110

Tabel 12. 2: Contoh Hasil *Gap Analysis* 111

Tabel 12. 3: Atribut Minimum Inventaris Sistem AI 112

Tabel 12. 4: Contoh Klasifikasi Risiko Awal Sistem AI 112

Tabel 12. 5: Hierarki Dokumen AIMS..... 113

Tabel 12. 6: Keluaran Peta Jalan 30–60–90 Hari 116

Tabel 12. 7: Tantangan Implementasi dan Strategi Mengatasinya.. 117

Tabel 12. 8: <i>Checklist</i> Evaluasi Bab 12	117
Tabel 13. 1: Contoh Objek Pemantauan dan Pengukuran AIMS.....	118
Tabel 13. 2: Contoh Program Audit Internal AIMS Tahunan	119
Tabel 13. 3: Teknik Audit untuk Sistem AI	120
Tabel 13. 4: Masukan dan Keluaran Tinjauan Manajemen	120
Tabel 13. 5: Perbandingan Audit Tahap 1 dan Tahap 2	122
Tabel 13. 6: Klasifikasi Temuan Audit	123
Tabel 13. 7: <i>Checklist</i> Evaluasi Bab 13	123
Tabel 14. 1: Studi Kasus AI pada SOC.....	125
Tabel 14. 2: Studi Kasus Deteksi Intrusi Berbasis AI	126
Tabel 14. 3: Studi Kasus Deteksi <i>Phishing</i> dan <i>Malware</i>	126
Tabel 14. 4: Studi Kasus AI untuk Pengujian Penetrasi.....	127
Tabel 14. 5: Studi Kasus Kebocoran Data melalui GenAI.....	128
Tabel 14. 6: Studi Kasus <i>Prompt Injection</i> pada Chatbot	128
Tabel 14. 7: Studi Kasus Shadow AI	129
Tabel 14. 8: Studi Kasus AI untuk DLP	129
Tabel 14. 9: Studi Kasus AI untuk Pelindungan Data Pribadi.....	130
Tabel 14. 10: Studi Kasus AI Biometrik.....	130
Tabel 14. 11: Studi Kasus AI pada Fintech.....	131
Tabel 14. 12: Studi Kasus AI pada Layanan Kesehatan	132
Tabel 14. 13: Pelajaran Utama dari Studi Kasus	132
Tabel 14. 14: <i>Checklist</i> Evaluasi Bab 14.....	133
Tabel 15. 1: Karakteristik Tingkat Kematangan AIMS	135
Tabel 15. 2: <i>Checklist</i> Evaluasi Bab 15	138
Tabel L.A. 1: <i>Template</i> Inventaris Sistem AI.....	139
Tabel L.B. 1: <i>Template</i> AI Risk Register	141
Tabel L.C. 1: <i>Template</i> AI System Impact Assessment.....	142
Tabel L.D. 1: <i>Template</i> Kebijakan Kecerdasan Buatan	143
Tabel L.E. 1: <i>Template</i> AIMS Control Matrix.....	144
Tabel L.F. 1: <i>Template</i> AUP Generative AI.....	147
Tabel L.G. 1: <i>Checklist</i> Gap Analysis ISO/IEC 42001	148
Tabel L.H. 1: <i>Checklist</i> Internal Audit AIMS	150
Tabel L.I. 1: <i>Template</i> Privacy Impact Assessment untuk Sistem AI .	152
Tabel L.J. 1: Pemetaan AIMS, ISMS, dan Privasi.....	153

DAFTAR GAMBAR

Gambar 1. 1: Linimasa Perkembangan AI dan Tonggak Standardisasi	2
Gambar 1. 2: Hierarki AI, <i>Machine Learning</i> , <i>Deep Learning</i> , dan <i>Generative AI</i>	3
Gambar 2. 1: Struktur Klausul ISO/IEC 42001:2023 dalam Siklus PDCA.....	13
Gambar 2. 2: Ekosistem Standar ISO/IEC terkait Sistem Manajemen AI	19
Gambar 3. 1: Contoh Struktur Tata Kelola AI Organisasi	27
Gambar 4. 1: Proses Manajemen Risiko AI Berbasis ISO/IEC 23894	33
Gambar 4. 2: Contoh Heatmap Risiko AI 5×5	36
Gambar 5. 1: Spektrum Model Pengawasan Manusia terhadap Sistem AI	48
Gambar 6. 1: Siklus Hidup Sistem AI dan Aktivitas Data	51
Gambar 6. 2: Ilustrasi <i>Data Drift</i> dan <i>Model Drift</i>	58
Gambar 7. 1: Jumlah Kontrol per Area Annex A ISO/IEC 42001.....	61
Gambar 7. 2: Alur Pemilihan Kontrol dan Penyusunan SoA	67
Gambar 8. 1: Proses AI <i>System Impact Assessment</i> Berbasis ISO/IEC 42005	72
Gambar 9. 1: Permukaan Serangan pada Pipeline Sistem AI	82
Gambar 9. 2: Arsitektur Pemanfaatan AI pada <i>Security Operations</i> <i>Center</i>	87
Gambar 10. 1: Irisan AIMS, ISMS, dan PIMS dalam Tata Kelola Terintegrasi.....	91
Gambar 10. 2: <i>Privacy by Design</i> dan PET sepanjang <i>Pipeline AI</i>	96
Gambar 11. 1: <i>Loop AI Agent</i> dan Titik Kendali Keamanan.....	105
Gambar 11. 2: Arsitektur Referensi <i>Generative AI</i> yang Aman	108
Gambar 12. 1: Tahapan Implementasi AIMS	115
Gambar 12. 2: Contoh Peta Jalan Implementasi AIMS 90 Hari	116
Gambar 13. 1: Siklus Sertifikasi AIMS Tiga Tahun	122
Gambar 15. 1: Model Kematangan AIMS Lima Tingkat	135

BAB 1

PENDAHULUAN KECERDASAN BUATAN DAN AIMS

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu menjelaskan perkembangan kecerdasan buatan, membedakan *machine learning*, *deep learning*, *generative AI*, *LLM*, dan *AI agent*, mengenali risiko serta dampak AI bagi organisasi, dan memahami mengapa sistem manajemen kecerdasan buatan (AIMS) diperlukan.

A. Perkembangan Artificial Intelligence

Kecerdasan buatan (*Artificial Intelligence/AI*) telah berkembang dari gagasan akademik menjadi teknologi yang menopang layanan publik, industri keuangan, kesehatan, manufaktur, hingga operasi keamanan siber. Istilah AI mulai dikenal luas sejak Konferensi Dartmouth tahun 1956, ketika sekelompok peneliti mengajukan hipotesis bahwa setiap aspek pembelajaran dan kecerdasan dapat dideskripsikan secara presisi sehingga dapat disimulasikan oleh mesin. Sejak saat itu, AI melalui beberapa gelombang optimisme dan stagnasi yang sering disebut sebagai *AI winter*.

Gelombang pertama didominasi oleh pendekatan simbolik, yaitu sistem yang bekerja berdasarkan aturan dan logika yang ditulis oleh manusia. Pada dekade 1980-an, sistem pakar (*expert system*) banyak digunakan untuk diagnosis dan konfigurasi, namun kesulitan dalam memelihara ribuan aturan membuat pendekatan ini terbatas. Gelombang berikutnya datang dari pendekatan statistik dan *machine learning* yang memungkinkan mesin belajar dari data, kemudian dipercepat oleh ketersediaan data besar, komputasi GPU, dan arsitektur jaringan saraf dalam (*deep learning*) sejak awal 2010-an.

Tonggak penting berikutnya adalah arsitektur *Transformer* yang diperkenalkan oleh Vaswani dan kolega pada tahun 2017. Arsitektur ini menjadi fondasi *Large Language Model* (LLM) dan mendorong adopsi massal *Generative AI* sejak akhir 2022. Dalam waktu yang relatif singkat,

kemampuan AI untuk menulis, meringkas, menerjemahkan, menghasilkan kode, dan menganalisis dokumen berpindah dari laboratorium ke meja kerja karyawan di hampir semua sektor.

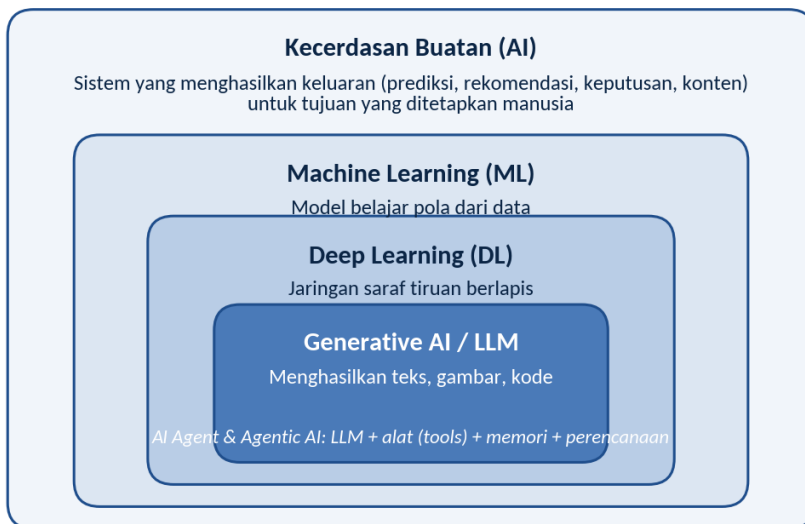


Gambar 1. 1: Linimasa Perkembangan AI dan Tonggak Standardisasi
Sumber: Diolah Penulis

Perkembangan teknologi tersebut diikuti oleh respons regulasi dan standardisasi. Pada Desember 2023, ISO dan IEC menerbitkan ISO/IEC 42001:2023 sebagai standar sistem manajemen AI pertama yang dapat disertifikasi. Uni Eropa mengesahkan *Artificial Intelligence Act* pada tahun 2024, sedangkan di Indonesia telah terbit Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang relevan bagi setiap sistem AI yang memproses data pribadi.

B. Machine Learning, Deep Learning, dan Generative AI

ISO/IEC 22989:2022 mendefinisikan sistem AI sebagai sistem rekayasa yang menghasilkan keluaran seperti konten, prakiraan, rekomendasi, atau keputusan untuk sekumpulan tujuan yang ditetapkan manusia. Definisi ini penting karena menempatkan tujuan dan tanggung jawab tetap pada manusia dan organisasi, bukan pada mesin. Di dalam payung AI terdapat beberapa pendekatan yang saling bertingkat seperti ditunjukkan pada Gambar 1.2.



Gambar 1. 2: Hierarki AI, *Machine Learning*, *Deep Learning*, dan *Generative AI*

Sumber: Diolah Penulis

Machine learning (ML) adalah proses mengoptimalkan parameter model melalui teknik komputasi sehingga perilaku model mencerminkan data atau pengalaman. Berbeda dengan perangkat lunak konvensional yang logikanya ditulis secara eksplisit, perilaku model ML sangat bergantung pada kualitas dan representativitas data latih. Karakteristik inilah yang menimbulkan kebutuhan pengendalian khusus, misalnya terhadap bias data, pergeseran distribusi data (*data drift*), dan keterjelasan (*explainability*) keputusan model.

Tabel 1. 1: Jenis Pendekatan *Machine Learning*

Pendekatan	Cara Kerja	Contoh Penerapan Keamanan
<i>Supervised learning</i>	Belajar dari data berlabel untuk memetakan masukan ke keluaran	Klasifikasi email <i>phishing</i> , deteksi <i>malware</i>
<i>Unsupervised learning</i>	Menemukan pola atau kelompok tanpa label	Deteksi anomali lalu lintas jaringan, UEBA
<i>Semi-supervised learning</i>	Memadukan sedikit data berlabel dengan banyak data tak berlabel	Triase alert SOC dengan label analisis terbatas

Pendekatan	Cara Kerja	Contoh Penerapan Keamanan
<i>Reinforcement learning</i>	Belajar dari imbalan (<i>reward</i>) atas tindakan	Optimasi respons otomatis, simulasi serangan
<i>Transfer learning</i>	Memanfaatkan model pralatih untuk tugas baru	Adaptasi LLM untuk analisis log

Sumber: Diolah Penulis

Deep learning merupakan bagian dari ML yang menggunakan jaringan saraf tiruan berlapis banyak untuk mempelajari representasi data yang kompleks seperti citra, suara, dan bahasa. Kemampuannya sangat tinggi, tetapi model *deep learning* umumnya bersifat kotak hitam (*black box*) sehingga menyulitkan audit dan penjelasan keputusan. *Generative AI* adalah kelas model yang mampu menghasilkan konten baru berupa teks, gambar, audio, video, atau kode berdasarkan pola yang dipelajari. Kemampuan generatif membuka manfaat produktivitas yang besar, sekaligus risiko baru seperti halusinasi, kebocoran data melalui *prompt*, dan penyalahgunaan untuk rekayasa sosial.

C. *Large Language Model, AI Agent, dan Agentic AI*

Large Language Model (LLM) adalah model bahasa berukuran sangat besar yang dilatih dengan korpus teks masif untuk memprediksi token berikutnya. Melalui proses penyelarasan (*alignment*) dan penyetelan instruksi, LLM mampu mengikuti perintah dalam bahasa alami. LLM dapat digunakan langsung melalui antarmuka percakapan, diintegrasikan melalui API, atau diperkaya dengan data internal organisasi melalui teknik *Retrieval-Augmented Generation* (RAG).

ISO/IEC 22989:2022 menjelaskan konsep agen sebagai entitas yang memersepsikan lingkungannya dan bertindak untuk mencapai tujuan. Dalam konteks terkini, *AI agent* adalah sistem berbasis LLM yang tidak hanya menjawab, tetapi juga merencanakan langkah, memanggil alat (*tools*) seperti API, basis data, peramban, atau skrip, lalu mengevaluasi hasilnya. *Agentic AI* merujuk pada arsitektur yang memberi agen tingkat otonomi lebih tinggi, termasuk kemampuan menjalankan rangkaian tugas multi-langkah dan berkolaborasi dengan agen lain.

Tabel 1. 2: Perbandingan *Chatbot* LLM, Aplikasi RAG, dan AI *Agent*

Aspek	<i>Chatbot</i> LLM	Aplikasi RAG	AI <i>Agent</i> / <i>Agentic</i> AI
Fungsi utama	Menjawab dan menghasilkan teks	Menjawab berbasis dokumen organisasi	Merencanakan dan mengeksekusi tindakan
Akses data	Data latih model	Data latih + basis pengetahuan internal	Data internal, API, sistem operasional
Tingkat otonomi	Rendah	Rendah-sedang	Sedang-tinggi
Risiko dominan	Halusinasi, kebocoran <i>prompt</i>	Kebocoran dokumen, <i>indirect prompt injection</i>	Aksi tidak sah, eskalasi hak akses, dampak berantai
Kontrol kunci	Kebijakan penggunaan, filter keluaran	ACL dokumen, sanitasi sumber, sitasi	<i>Least privilege</i> , persetujuan manusia, <i>sandbox</i> , log jejak

Sumber: Diolah Penulis

Perbedaan tingkat otonomi tersebut berimplikasi langsung pada desain kontrol. Semakin tinggi kemampuan sistem untuk bertindak atas nama organisasi, semakin penting pengawasan manusia (*human oversight*), pembatasan hak akses, dan pencatatan jejak keputusan agar setiap tindakan dapat ditelusuri dan dipertanggungjawabkan.

D. Pemanfaatan AI dalam Organisasi

Organisasi memanfaatkan AI untuk meningkatkan efisiensi, kualitas keputusan, dan pengalaman pelanggan. Di sektor keuangan, AI digunakan untuk penilaian kredit, deteksi *fraud*, dan asisten virtual. Di sektor kesehatan, AI membantu analisis citra medis dan triase pasien. Di sektor pemerintahan, AI mendukung layanan informasi publik dan analisis kebijakan. Di bidang keamanan siber, AI menjadi komponen penting dalam deteksi ancaman, analisis *malware*, dan otomasi pusat operasi keamanan (*Security Operations Center/SOC*).

Tabel 1. 3: Contoh Pemanfaatan AI Lintas Sektor

Sektor	Contoh Pemanfaatan	Isu Tata Kelola Utama
Perbankan & <i>fintech</i>	<i>Credit scoring</i> , deteksi <i>fraud</i> , <i>chatbot</i> layanan	Keadilan keputusan, penjelasan penolakan, PDP
Kesehatan	Analisis citra, ringkasan rekam medis, triase	Keselamatan pasien, data kesehatan sebagai data spesifik
Pemerintahan	Layanan informasi publik, analisis dokumen	Transparansi, akuntabilitas, dampak sosial
Manufaktur & energi	<i>Predictive maintenance</i> , kontrol kualitas visual	Keselamatan operasi, ketahanan sistem
Keamanan siber	Deteksi anomali, triase alert, analisis <i>phishing</i>	<i>False negative</i> , serangan adversarial terhadap model
Sumber daya manusia	Penyaringan CV, analitik kinerja	Bias dan diskriminasi, privasi karyawan

Sumber: Diolah Penulis

Pemanfaatan AI tidak selalu berbentuk pengembangan model sendiri. Banyak organisasi berperan sebagai pengguna layanan AI pihak ketiga, misalnya menggunakan asisten AI pada aplikasi perkantoran atau *platform* SaaS. Peran tersebut tetap membawa kewajiban tata kelola, karena organisasi bertanggung jawab atas data yang dimasukkan, keputusan yang diambil berdasarkan keluaran AI, dan dampaknya terhadap pelanggan maupun karyawan.

E. Risiko dan Dampak *Artificial intelligence*

AI membawa risiko yang berbeda dari teknologi informasi konvensional. Perilaku sistem dipelajari dari data, dapat berubah seiring waktu, sering sulit dijelaskan, dan dapat memengaruhi hak serta kesempatan individu. ISO/IEC 23894:2023 menegaskan bahwa AI dapat memunculkan risiko baru atau mengubah kemungkinan risiko yang sudah ada, baik dengan konsekuensi positif maupun negatif terhadap sasaran organisasi.

Tabel 1. 4: Kategori Risiko dan Dampak AI

Kategori	Contoh Risiko	Pihak Terdampak
Teknis	Halusinasi, <i>model drift</i> , kegagalan generalisasi	Organisasi, pengguna

Kategori	Contoh Risiko	Pihak Terdampak
Keamanan siber	<i>Prompt injection, data poisoning, model extraction</i>	Organisasi, pelanggan
Privasi	Kebocoran data pribadi, inferensi atribut sensitif	Subjek data
Etika & sosial	Bias, diskriminasi, manipulasi, disinformasi	Individu, kelompok, masyarakat
Hukum & kepatuhan	Pelanggaran UU PDP, hak kekayaan intelektual	Organisasi
Operasional	Ketergantungan vendor, <i>shadow AI</i> , kurangnya kompetensi	Organisasi
Lingkungan	Konsumsi energi pelatihan dan inferensi	Masyarakat

Sumber: Diolah Penulis

Laporan *Cost of a Data Breach 2024* yang dirilis IBM mencatat rata-rata biaya global pelanggaran data mencapai sekitar USD 4,88 juta per insiden. Angka ini menunjukkan bahwa kegagalan mengelola data, termasuk data yang mengalir ke sistem AI, memiliki konsekuensi finansial yang nyata. Di sisi lain, dampak AI tidak hanya dirasakan oleh organisasi. Keputusan kredit yang bias, sistem pengenalan wajah yang salah mengidentifikasi, atau informasi keliru dari *chatbot* layanan publik dapat merugikan individu dan kelompok masyarakat yang tidak memiliki kendali atas sistem tersebut.

F. AI Governance dan Responsible AI

Tata kelola AI (*AI governance*) adalah sistem pengarahan, pengendalian, dan akuntabilitas atas pengembangan, pengadaan, dan penggunaan AI di organisasi. ISO/IEC 38507:2022 menjelaskan implikasi tata kelola bagi badan pengarah (*governing body*) ketika organisasi menggunakan AI, termasuk perlunya kebijakan baru, penyesuaian selera risiko, dan pengawasan penggunaan yang bertanggung jawab. Tata kelola memastikan AI dimanfaatkan sesuai nilai organisasi, peraturan, dan harapan pemangku kepentingan.

Responsible AI adalah pendekatan yang memastikan AI dikembangkan dan digunakan secara adil, transparan, aman, menghormati privasi, dan dapat dipertanggungjawabkan. Berbagai

kerangka internasional merumuskan prinsip yang saling beririsan, sebagaimana dirangkum pada Tabel 1.5.

Tabel 1. 4: Prinsip *Responsible AI* dari Beberapa Kerangka Rujukan

Kerangka	Prinsip Utama
Rekomendasi OECD tentang AI (2019, diperbarui 2024)	Pertumbuhan inklusif dan kesejahteraan; nilai hak asasi dan demokrasi termasuk keadilan dan privasi; transparansi dan keterjelasan; ketahanan, keamanan, dan keselamatan; akuntabilitas
Rekomendasi UNESCO tentang Etika AI (2021)	Proporsionalitas dan tidak merugikan; keselamatan dan keamanan; privasi; tata kelola adaptif; tanggung jawab; transparansi; kesadaran publik; keadilan dan non-diskriminasi; keberlanjutan
NIST AI RMF 1.0 (2023)	Valid dan andal; aman; tangguh dan terlindungi; akuntabel dan transparan; dapat dijelaskan dan diinterpretasikan; meningkatkan privasi; adil dengan bias berbahaya yang dikelola
SE Menkominfo No. 9 Tahun 2023	Inklusivitas, kemanusiaan, keamanan, aksesibilitas, transparansi, kredibilitas dan akuntabilitas, perlindungan data pribadi, keberlanjutan, dan kekayaan intelektual

Sumber: Diolah Penulis

Prinsip-prinsip tersebut bernilai penting sebagai arah, tetapi organisasi memerlukan mekanisme yang lebih konkret agar prinsip dapat diterapkan secara konsisten, diukur, dan diaudit. Kebutuhan inilah yang dijawab oleh pendekatan sistem manajemen.

G. Artificial Intelligence Management System

Artificial Intelligence Management System (AIMS) atau sistem manajemen kecerdasan buatan adalah sekumpulan elemen organisasi yang saling terkait, meliputi kebijakan, sasaran, proses, peran, sumber daya, dan kontrol, untuk mengelola pengembangan, penyediaan, dan penggunaan sistem AI secara bertanggung jawab. ISO/IEC 42001:2023 menetapkan persyaratan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan AIMS dalam konteks organisasi.

Pendekatan sistem manajemen memberikan beberapa keunggulan. Pertama, prinsip *responsible AI* diterjemahkan menjadi proses yang berulang, misalnya penilaian risiko AI, penilaian dampak sistem AI, dan pengendalian siklus hidup. Kedua, tanggung jawab dialokasikan secara

jelas dari pimpinan puncak hingga pemilik sistem. Ketiga, efektivitas dapat dibuktikan melalui informasi terdokumentasi, audit internal, dan tinjauan manajemen. Keempat, AIMS dapat diintegrasikan dengan sistem manajemen yang sudah berjalan, terutama sistem manajemen keamanan informasi (ISMS) ISO/IEC 27001 dan sistem manajemen informasi privasi (PIMS) ISO/IEC 27701.

Bagi organisasi di Indonesia, AIMS juga menjadi sarana praktis untuk menunjukkan kepatuhan terhadap kewajiban perlindungan data pribadi, pedoman etika AI, serta persyaratan sektor seperti panduan kode etik AI yang diterbitkan Otoritas Jasa Keuangan untuk industri teknologi finansial. Dengan demikian, AIMS bukan sekadar dokumen sertifikasi, melainkan kerangka kerja untuk membangun kepercayaan terhadap AI.

H. Tujuan dan Struktur Buku

Buku ini bertujuan menyediakan panduan praktis untuk memahami, membangun, menerapkan, memelihara, dan meningkatkan AIMS berbasis ISO/IEC 42001:2023, serta menerapkannya dalam keamanan informasi, keamanan siber, dan perlindungan data pribadi. Pendekatan yang digunakan adalah berbasis risiko, berbasis siklus hidup, berbasis kontrol, *security by design*, *privacy by design*, dan *responsible AI*. Nomor klausul dan kontrol yang dirujuk dalam buku ini disajikan dalam bentuk uraian dan interpretasi penulis; pembaca tetap perlu merujuk teks resmi standar untuk keperluan kepatuhan dan sertifikasi.

Tabel 1. 5: Struktur Isi Buku

Bagian	Cakupan
Bab 1–3	Fondasi AI, pemahaman ISO/IEC 42001:2023, konteks organisasi, dan tata kelola AI
Bab 4–7	Perencanaan dan manajemen risiko AI, dukungan dan operasional, siklus hidup dan tata kelola data, serta kontrol Annex A
Bab 8–10	Penilaian dampak dan <i>responsible AI</i> , AI dalam keamanan informasi dan siber, integrasi AIMS dengan ISMS dan perlindungan data pribadi
Bab 11	Keamanan <i>Generative AI</i> , LLM, RAG, dan <i>AI agent</i>
Bab 12–14	Implementasi AIMS, audit dan sertifikasi, serta studi kasus lintas sektor

Bagian	Cakupan
Bab 15	Kesimpulan, model kematangan, dan rekomendasi
Lampiran	Template siap pakai: inventaris AI, <i>risk register</i> , AIIA, kebijakan AI, matriks kontrol, AUP GenAI, <i>checklist</i> audit, PIA, dan pemetaan AIMS-ISMS-privasi

Sumber: Diolah Penulis

I. Ringkasan dan *Checklist* Evaluasi

AI telah berkembang menjadi teknologi strategis yang membawa manfaat besar sekaligus risiko teknis, keamanan, privasi, etika, dan hukum. Perbedaan karakter AI dibandingkan dengan perangkat lunak konvensional, terutama ketergantungan pada data, sifat adaptif, dan dampaknya terhadap individu, menuntut tata kelola khusus. ISO/IEC 42001:2023 menyediakan kerangka sistem manajemen untuk menerjemahkan prinsip *responsible AI* menjadi praktik yang terukur dan dapat diaudit.

Tabel 1. 6: *Checklist* Evaluasi Bab 1

No	Pertanyaan Evaluasi	Status
1	Apakah organisasi telah memahami perbedaan AI, ML, <i>deep learning</i> , <i>generative AI</i> , dan <i>AI agent</i> yang digunakannya?	Ya / Belum
2	Apakah pemanfaatan AI di organisasi telah diidentifikasi, termasuk layanan AI pihak ketiga?	Ya / Belum
3	Apakah risiko teknis, keamanan, privasi, dan etika AI telah dikenali oleh manajemen?	Ya / Belum
4	Apakah prinsip <i>responsible AI</i> yang dianut organisasi telah ditetapkan?	Ya / Belum
5	Apakah manajemen memahami manfaat penerapan AIMS berbasis ISO/IEC 42001?	Ya / Belum

Sumber: Diolah Penulis

Pembahasan pada bab berikutnya menguraikan latar belakang, struktur, dan prinsip ISO/IEC 42001:2023 secara lebih rinci sebagai landasan penerapan AIMS.

BAB 2

MEMAHAMI ISO/IEC 42001:2023

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu menjelaskan latar belakang dan manfaat ISO/IEC 42001:2023, memahami struktur klausul dan lampiran standar, mengenali peran pemangku kepentingan AI, serta memahami hubungan AIMS dengan sistem manajemen lain dan proses sertifikasinya.

A. Latar Belakang ISO/IEC 42001

ISO/IEC 42001:2023 *Information technology (Artificial intelligence) Management system* diterbitkan pada Desember 2023 sebagai edisi pertama. Standar ini disusun oleh *Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 42 Artificial Intelligence*, yaitu komite yang juga menghasilkan standar konsep dan terminologi AI (ISO/IEC 22989), kerangka sistem AI berbasis ML (ISO/IEC 23053), pedoman manajemen risiko AI (ISO/IEC 23894), dan penilaian dampak sistem AI (ISO/IEC 42005).

Kehadiran ISO/IEC 42001 dilatarbelakangi oleh kebutuhan organisasi akan kerangka yang dapat diterapkan secara universal untuk mengelola AI secara bertanggung jawab. Sebelum standar ini terbit, organisasi umumnya bergantung pada pedoman etika yang bersifat prinsip, kebijakan internal yang beragam, atau regulasi sektoral yang belum lengkap. Pedoman seperti itu sulit diaudit dan tidak memberikan jaminan konsistensi penerapan. ISO/IEC 42001 menjembatani kesenjangan tersebut dengan menyediakan persyaratan yang terstruktur, dapat diverifikasi, dan dapat disertifikasi oleh pihak ketiga.

Standar ini berlaku untuk semua organisasi, tanpa memandang ukuran, jenis, maupun sifatnya, yang menyediakan atau menggunakan produk dan layanan berbasis sistem AI. Dengan kata lain, organisasi yang

hanya menggunakan layanan AI pihak ketiga pun dapat menerapkan AIMS, tidak terbatas pada perusahaan teknologi yang mengembangkan model. ISO/IEC 42001 menggunakan struktur harmonis (*harmonized structure*) yang sama dengan standar sistem manajemen ISO lainnya, sehingga mudah diintegrasikan dengan ISO/IEC 27001, ISO 9001, atau ISO/IEC 27701.

B. Tujuan dan Manfaat AIMS

Tujuan utama AIMS adalah membantu organisasi mengembangkan, menyediakan, atau menggunakan sistem AI secara bertanggung jawab dalam mencapai sasarannya, sambil memenuhi persyaratan yang berlaku, kewajiban kepada pihak berkepentingan, dan harapan mereka. AIMS memastikan bahwa risiko dan peluang AI dikelola secara sistematis sepanjang siklus hidup sistem.

Tabel 2. 1: Manfaat Penerapan AIMS bagi Organisasi

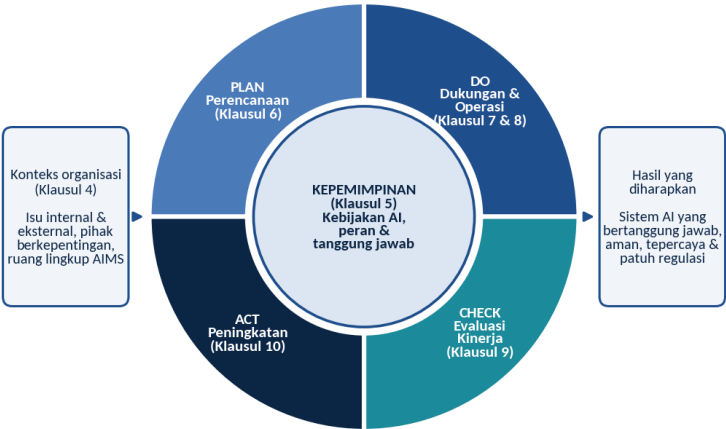
Manfaat	Uraian
Kepercayaan pemangku kepentingan	Menunjukkan bahwa AI dikembangkan dan digunakan secara bertanggung jawab, transparan, dan akuntabel
Pengelolaan risiko terstruktur	Risiko AI terhadap organisasi, individu, dan masyarakat diidentifikasi, dianalisis, dan ditangani secara konsisten
Kepatuhan regulasi	Mendukung pemenuhan UU PDP, pedoman etika AI nasional, regulasi sektor, serta regulasi internasional seperti EU AI Act
Keunggulan kompetitif	Sertifikasi AIMS menjadi pembeda dalam pengadaan dan kerja sama dengan mitra global
Efisiensi dan integrasi	Memanfaatkan struktur yang sama dengan ISMS dan PIMS sehingga dokumentasi, audit, dan tinjauan dapat digabung
Inovasi yang terkendali	Memberi pagar pengaman (<i>guardrail</i>) agar organisasi dapat berinovasi dengan AI tanpa mengabaikan dampak

Sumber: Diolah Penulis

Manfaat tersebut hanya dapat diperoleh apabila AIMS diterapkan secara substantif. Organisasi yang sekadar menyiapkan dokumen untuk sertifikasi tanpa mengubah praktik pengembangan dan penggunaan AI akan menghadapi temuan audit, sekaligus tetap terpapar risiko nyata.

C. Struktur ISO/IEC 42001:2023

ISO/IEC 42001:2023 terdiri atas sepuluh klausul dan empat lampiran. Klausul 1 sampai 3 bersifat pengantar, sedangkan klausul 4 sampai 10 memuat persyaratan sistem manajemen yang harus dipenuhi apabila organisasi mengklaim kesesuaian. Struktur ini mengikuti siklus *Plan-Do-Check-Act* (PDCA) seperti ditunjukkan pada Gambar 2.1.



Gambar 2. 1: Struktur Klausul ISO/IEC 42001:2023 dalam Siklus PDCA

Sumber: Diolah Penulis

Tabel 2. 2: Struktur Klausul ISO/IEC 42001:2023

Klausul	Judul	Pokok Persyaratan
1–3	Ruang lingkup, acuan normatif, istilah dan definisi	Batas penerapan standar, rujukan ISO/IEC 22989, serta istilah yang digunakan
4	Konteks organisasi	Isu internal dan eksternal, peran organisasi terhadap AI, pihak berkepentingan, ruang lingkup AIMS
5	Kepemimpinan	Komitmen manajemen puncak, kebijakan AI, peran, tanggung jawab, dan wewenang
6	Perencanaan	Risiko dan peluang, penilaian dan perlakuan risiko AI, penilaian dampak sistem AI, sasaran AI, perencanaan perubahan
7	Dukungan	Sumber daya, kompetensi, kesadaran, komunikasi, informasi terdokumentasi

Klausul	Judul	Pokok Persyaratan
8	Operasi	Perencanaan dan pengendalian operasional, pelaksanaan penilaian risiko, perlakuan risiko, dan penilaian dampak
9	Evaluasi kinerja	Pemantauan dan pengukuran, audit internal, tinjauan manajemen
10	Peningkatan	Peningkatan berkelanjutan, ketidaksesuaian dan tindakan korektif

Sumber: Diolah Penulis

Selain klausul utama, standar ini memiliki empat lampiran. *Annex A* (normatif) memuat 38 kontrol acuan yang dikelompokkan ke dalam sembilan area sasaran kontrol. *Annex B* (normatif) memberikan panduan implementasi untuk setiap kontrol. *Annex C* (informatif) memberikan contoh sasaran organisasi terkait AI dan sumber risiko AI. *Annex D* (informatif) menjelaskan penggunaan AIMS lintas domain dan sektor, termasuk integrasi dengan standar sistem manajemen lain.

Tabel 2. 3: Lampiran ISO/IEC 42001:2023

Lampiran	Isi
<i>Annex A</i> (normatif)	Sasaran kontrol dan kontrol acuan: kebijakan AI, organisasi internal, sumber daya, penilaian dampak, siklus hidup, data, informasi bagi pihak berkepentingan, penggunaan AI, serta hubungan pihak ketiga dan pelanggan
<i>Annex B</i> (normatif)	Panduan implementasi kontrol Annex A, termasuk contoh isi kebijakan, dokumentasi, dan praktik
<i>Annex C</i> (informatif)	Contoh sasaran organisasi (akuntabilitas, keahlian AI, kualitas data, dampak lingkungan, keadilan, keterpeliharaan, privasi, ketangguhan, keselamatan, keamanan, transparansi) dan sumber risiko AI
<i>Annex D</i> (informatif)	Penggunaan AIMS lintas domain dan sektor serta integrasi dengan ISO/IEC 27001, ISO/IEC 27701, ISO 9001, dan standar sektoral

Sumber: Diolah Penulis

Pemahaman terhadap istilah kunci sangat penting karena standar ini menggunakan terminologi yang presisi. Tabel 2.4 merangkum beberapa istilah yang paling sering muncul dalam penerapan.

Tabel 2. 4: Istilah Kunci dalam Penerapan AIMS

Istilah	Pengertian Ringkas
Sistem AI	Sistem rekayasa yang menghasilkan keluaran seperti konten, prakiraan, rekomendasi, atau keputusan untuk tujuan yang ditetapkan manusia
Pihak berkepentingan	Orang atau organisasi yang dapat memengaruhi, dipengaruhi, atau merasa dipengaruhi oleh keputusan atau aktivitas terkait AI
Penilaian dampak sistem AI	Proses formal untuk mengidentifikasi, mengevaluasi, dan menangani dampak sistem AI terhadap individu, kelompok, dan masyarakat
<i>Statement of Applicability</i> (SoA)	Dokumen yang memuat kontrol yang diperlukan beserta justifikasi inklusi dan eksklusinya
Kualitas data	Karakteristik data yang menunjukkan kemampuan data memenuhi kebutuhan organisasi dalam konteks tertentu
Informasi terdokumentasi	Informasi yang harus dikendalikan dan dipelihara organisasi beserta media penyimpanannya
Ketidaksesuaian	Tidak terpenuhinya suatu persyaratan

Sumber: Diolah Penulis

D. Prinsip Sistem Manajemen AI

Penerapan AIMS bertumpu pada beberapa prinsip sistem manajemen yang saling melengkapi. Prinsip pertama adalah pendekatan proses, yaitu memandang pengelolaan AI sebagai rangkaian proses yang saling terkait dengan masukan, keluaran, pemilik, dan indikator kinerja. Prinsip kedua adalah pemikiran berbasis risiko (*risk-based thinking*), yaitu setiap keputusan terkait AI mempertimbangkan risiko dan peluang secara proporsional terhadap dampaknya.

Prinsip ketiga adalah siklus PDCA untuk peningkatan berkelanjutan. Prinsip keempat adalah kepemimpinan, karena tanpa komitmen manajemen puncak, AIMS akan berhenti sebagai proyek dokumentasi. Prinsip kelima adalah pengambilan keputusan berbasis bukti melalui pemantauan, pengukuran, dan audit. Selain prinsip generik tersebut, AIMS memiliki prinsip khas AI yang tercermin dalam sasaran pada *Annex C*, seperti keadilan, transparansi, keterjelasan, ketangguhan, keselamatan, keamanan, privasi, dan akuntabilitas.

Tabel 2. 5: Prinsip Sistem Manajemen dan Penerapannya pada AI

Prinsip	Makna dalam AIMS	Contoh Bukti
Pendekatan proses	Siklus hidup AI dikelola sebagai proses terkendali	Prosedur pengembangan dan <i>deployment</i> AI
Berbasis risiko	Kontrol dipilih sesuai tingkat risiko dan dampak	<i>AI risk register</i> , SoA
PDCA	Kinerja AIMS dievaluasi dan ditingkatkan	Laporan audit internal, notulen tinjauan manajemen
Kepemimpinan	Pimpinan menetapkan arah dan sumber daya	Kebijakan AI yang disahkan, SK komite AI
Berbasis bukti	Keputusan didasarkan pada data pemantauan	Dasbor KPI/KRI model dan insiden
<i>Responsible AI</i>	Nilai etis menjadi sasaran yang terukur	Laporan penilaian dampak, metrik <i>fairness</i>

Sumber: Diolah Penulis

E. Peran AI Provider, Developer, Producer, dan User

Salah satu keunikan ISO/IEC 42001 adalah persyaratan bagi organisasi untuk menentukan perannya terhadap sistem AI. Klausul 4.1 meminta organisasi mempertimbangkan peran tersebut ketika memahami konteksnya, karena kewajiban dan kontrol yang relevan berbeda antara organisasi yang mengembangkan model, yang menyediakan layanan AI, dan yang sekadar menggunakan AI. Rujukan peran tersebut dijabarkan dalam ISO/IEC 22989:2022.

Tabel 2. 6: Peran Pemangku Kepentingan AI Menurut ISO/IEC 22989

Peran	Deskripsi	Contoh
<i>AI provider</i>	Pihak yang menyediakan produk atau layanan yang menggunakan satu atau lebih sistem AI, termasuk penyedia <i>platform</i> AI	Penyedia layanan LLM melalui API, penyedia <i>platform</i> ML berbasis <i>cloud</i>
<i>AI producer</i>	Pihak yang merancang, mengembangkan, menguji, dan menerapkan produk atau layanan AI; mencakup <i>AI developer</i>	Tim internal yang membangun model deteksi <i>fraud</i>

Peran	Deskripsi	Contoh
<i>AI customer</i>	Pihak yang menggunakan produk atau layanan AI, secara langsung atau melalui penyedia; mencakup <i>AI user</i>	Bank yang memakai layanan <i>chatbot</i> pihak ketiga
<i>AI partner</i>	Pihak yang memberikan layanan terkait AI seperti integrator sistem, penyedia data, auditor, dan evaluator AI	Vendor pelabelan data, konsultan, auditor AIMS
<i>AI subject</i>	Pihak yang terdampak sistem AI, termasuk subjek data	Nasabah yang dinilai kreditnya oleh model
Otoritas terkait	Pembuat kebijakan dan regulator	Kementerian, OJK, lembaga perlindungan data pribadi

Sumber: Diolah Penulis

Satu organisasi dapat memegang beberapa peran sekaligus. Sebagai contoh, perusahaan teknologi finansial dapat menjadi *AI customer* ketika menggunakan layanan LLM dari penyedia global, sekaligus *AI producer* ketika mengembangkan model *credit scoring* sendiri, dan *AI provider* ketika menawarkan layanan penilaian kredit kepada mitra. Penetapan peran yang tepat menentukan kontrol Annex A yang relevan dan pembagian tanggung jawab dengan pihak ketiga sebagaimana diatur dalam kontrol A.10.

F. *Responsible Development* dan *Responsible Use*

ISO/IEC 42001 membedakan dua dimensi tanggung jawab, yaitu pengembangan yang bertanggung jawab (*responsible development*) dan penggunaan yang bertanggung jawab (*responsible use*). Dimensi pengembangan tercermin dalam kontrol A.6 tentang siklus hidup sistem AI, yang meminta organisasi menetapkan sasaran dan proses untuk desain dan pengembangan AI yang bertanggung jawab, termasuk persyaratan, verifikasi dan validasi, *deployment*, pemantauan, serta dokumentasi teknis.

Dimensi penggunaan tercermin dalam kontrol A.9, yang meminta organisasi menetapkan proses dan sasaran untuk penggunaan AI yang bertanggung jawab, serta memastikan sistem AI digunakan sesuai tujuan penggunaannya (*intended use*). Dimensi ini sangat relevan bagi

organisasi pengguna AI generatif, karena risiko utama sering muncul dari cara karyawan menggunakan alat AI, bukan dari model itu sendiri.

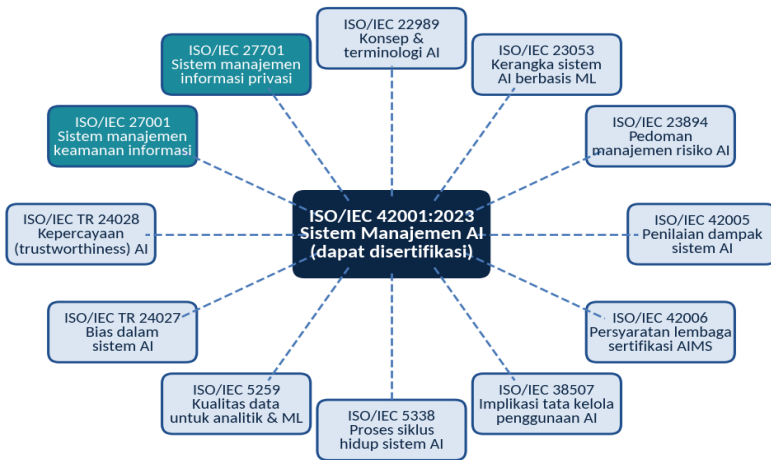
Tabel 2. 7: Perbandingan *Responsible Development* dan *Responsible Use*

Aspek	<i>Responsible Development</i>	<i>Responsible Use</i>
Fokus	Desain, pelatihan, validasi, dan rilis sistem AI	Pemanfaatan sistem AI dalam proses bisnis
Kontrol utama	A.6.1 dan A.6.2, A.7 (data)	A.9, A.8 (informasi bagi pengguna)
Pertanyaan kunci	Apakah model memenuhi persyaratan kinerja, keadilan, dan keamanan?	Apakah AI dipakai sesuai tujuan dan dengan pengawasan memadai?
Contoh bukti	Spesifikasi persyaratan, laporan pengujian, <i>model card</i>	Kebijakan penggunaan, log penggunaan, pelatihan pengguna

Sumber: Diolah Penulis

G. Hubungan ISO/IEC 42001 dengan Sistem Manajemen Lain

AIMS tidak berdiri sendiri. Annex D ISO/IEC 42001 menjelaskan bahwa organisasi yang menyediakan atau menggunakan AI umumnya juga memiliki sasaran keamanan, privasi, dan mutu yang menjadi fokus standar lain. Karena menggunakan struktur harmonis, AIMS dapat diintegrasikan dengan ISMS berbasis ISO/IEC 27001, PIMS berbasis ISO/IEC 27701, dan sistem manajemen mutu ISO 9001, bahkan dengan standar sektoral seperti ISO 13485 untuk perangkat medis.



Gambar 2. 2: Ekosistem Standar ISO/IEC terkait Sistem Manajemen AI

Sumber: Diolah Penulis

Dalam praktik, integrasi dilakukan melalui kebijakan terpadu, metodologi risiko yang selaras, satu program audit internal, serta tinjauan manajemen gabungan. Kontrol keamanan pada AIMS, misalnya pencatatan log sistem AI dan keamanan data, dapat diimplementasikan bersama kontrol ISO/IEC 27002, sedangkan kontrol terkait data pribadi dan penilaian dampak terhadap individu dapat diselaraskan dengan PIMS dan kewajiban UU PDP.

Tabel 2. 8: Integrasi AIMS dengan Standar Sistem Manajemen Lain

Standar	Titik Integrasi	Manfaat
ISO/IEC 27001	Metodologi risiko, kontrol keamanan, manajemen insiden, audit	Keamanan data, model, dan <i>pipeline</i> AI
ISO/IEC 27701	Pemrosesan data pribadi, penilaian dampak privasi	Kepatuhan UU PDP untuk sistem AI
ISO 9001	Pengendalian desain, pemasok, ketidaksesuaian	Mutu produk dan layanan berbasis AI
ISO 31000 / ISO/IEC 23894	Kerangka dan proses manajemen risiko	Konsistensi penilaian risiko AI
ISO/IEC 42005	Metode penilaian dampak sistem AI	Pelaksanaan kontrol A.5 yang lebih rinci

Sumber: Diolah Penulis

H. Sertifikasi ISO/IEC 42001

ISO/IEC 42001 dapat digunakan sebagai dasar sertifikasi pihak ketiga. Sertifikasi dilakukan oleh lembaga sertifikasi yang memenuhi persyaratan ISO/IEC 17021-1 dan, secara khusus untuk AIMS, ISO/IEC 42006:2025 yang menetapkan persyaratan tambahan bagi lembaga audit dan sertifikasi AIMS, termasuk kompetensi auditor di bidang AI. Keberadaan ISO/IEC 42006 penting untuk memastikan bahwa sertifikat AIMS diterbitkan oleh lembaga yang benar-benar memahami risiko teknis dan dampak AI.

Proses sertifikasi umumnya meliputi audit tahap 1 untuk menilai kesiapan dokumentasi dan ruang lingkup, audit tahap 2 untuk menilai efektivitas implementasi, keputusan sertifikasi, audit surveilans tahunan, dan resertifikasi pada tahun ketiga. Rincian proses ini dibahas pada Bab 13. Sertifikasi bukan tujuan akhir, tetapi bukti independen bahwa AIMS telah diterapkan dan dipelihara secara efektif.

I. Ringkasan dan *Checklist* Evaluasi

ISO/IEC 42001:2023 adalah standar sistem manajemen AI pertama yang dapat disertifikasi, disusun dengan struktur harmonis sehingga mudah diintegrasikan dengan ISMS dan PIMS. Standar ini mewajibkan organisasi untuk menentukan perannya terhadap AI, mengelola risiko dan dampak AI, memilih kontrol dari *Annex A* melalui SoA, serta mengevaluasi dan meningkatkan kinerja AIMS secara berkelanjutan.

Tabel 2. 9: Checklist Evaluasi Bab 2

No	Pertanyaan Evaluasi	Status
1	Apakah organisasi memahami struktur klausul 4–10 dan Annex A–D ISO/IEC 42001?	Ya / Belum
2	Apakah peran organisasi terhadap setiap sistem AI (<i>provider, producer, customer, partner</i>) telah ditetapkan?	Ya / Belum
3	Apakah dimensi <i>responsible development</i> dan <i>responsible use</i> telah dibedakan?	Ya / Belum
4	Apakah peluang integrasi dengan ISMS, PIMS, dan sistem manajemen lain telah dipetakan?	Ya / Belum
5	Apakah organisasi memahami persyaratan dan tahapan sertifikasi AIMS?	Ya / Belum

Sumber: Diolah Penulis

Bab berikutnya membahas penerapan klausul 4 dan 5, yaitu konteks organisasi, ruang lingkup AIMS, kepemimpinan, kebijakan AI, serta struktur tata kelola AI.

BAB 3

KONTEKS ORGANISASI DAN TATA KELOLA AI

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu menganalisis konteks internal dan eksternal yang relevan dengan AI, mengidentifikasi pihak berkepentingan, menetapkan ruang lingkup AIMS, menyusun kebijakan AI, serta merancang struktur tata kelola, peran, dan akuntabilitas AI.

A. Konteks Internal dan Eksternal

Klausul 4.1 ISO/IEC 42001 meminta organisasi menentukan isu eksternal dan internal yang relevan dengan tujuannya dan memengaruhi kemampuannya untuk mencapai hasil yang diharapkan dari AIMS. Organisasi juga perlu menentukan apakah perubahan iklim merupakan isu yang relevan, serta memahami tujuan penggunaan sistem AI yang dikembangkan, disediakan, atau digunakan. Analisis konteks menjadi fondasi untuk menetapkan ruang lingkup, kebijakan, dan kriteria risiko.

ISO/IEC 23894:2023 memberikan panduan tambahan tentang faktor konteks yang khas pada AI. Dalam konteks eksternal, organisasi perlu mempertimbangkan persyaratan hukum yang secara khusus berkaitan dengan AI, pedoman etika yang diterbitkan pemerintah maupun asosiasi industri, tren teknologi AI, persepsi pemangku kepentingan yang dapat dipengaruhi oleh kurangnya transparansi atau bias sistem, serta kompleksitas jaringan dan ketergantungan pada pihak ketiga. Dalam konteks internal, organisasi perlu mempertimbangkan budaya organisasi, kompetensi AI dan ilmu data, ketersediaan data, kekayaan intelektual, serta perubahan peran pekerjaan akibat otomatisasi.

BAB 4

PERENCANAAN DAN MANAJEMEN RISIKO AI

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu merancang proses penilaian dan perlakuan risiko AI sesuai klausul 6 ISO/IEC 42001 dan pedoman ISO/IEC 23894, menentukan tingkat risiko dan risiko residual, menyusun AI risk register, serta menetapkan sasaran AI beserta KPI dan KRI.

A. Risiko dan Peluang *Artificial Intelligence*

Klausul 6.1.1 ISO/IEC 42001 meminta organisasi mempertimbangkan isu konteks dan persyaratan pihak berkepentingan untuk menentukan risiko dan peluang yang perlu ditangani, agar AIMS mencapai hasil yang diharapkan, mencegah atau mengurangi efek yang tidak diinginkan, dan mencapai peningkatan berkelanjutan. Organisasi juga harus menetapkan kriteria risiko AI yang membedakan risiko yang dapat diterima dan yang tidak dapat diterima, serta kriteria untuk melakukan penilaian risiko, perlakuan risiko, dan penilaian dampak sistem AI.

Karakter risiko AI berbeda dari risiko TI konvensional. ISO/IEC 23894:2023 menekankan bahwa manajemen risiko AI harus dinamis karena sistem AI dapat terus belajar dan berubah, ekspektasi pelanggan berubah cepat, dan regulasi AI terus diperbarui. Selain itu, risiko AI tidak hanya berdampak pada organisasi, tetapi juga pada individu, kelompok, dan masyarakat. Oleh karena itu, kriteria risiko AI perlu mencakup dimensi dampak eksternal tersebut.

Peluang juga harus dikelola. Contoh peluang terkait AI adalah otomasi proses yang meningkatkan efisiensi, peningkatan kemampuan deteksi ancaman siber, serta peningkatan kualitas layanan pelanggan. Pengelolaan peluang memastikan organisasi tidak terjebak pada sikap terlalu menghindari risiko sehingga kehilangan manfaat strategis AI.

BAB 5

DUKUNGAN DAN OPERASIONAL SISTEM AI

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu menerapkan persyaratan dukungan (klausul 7) dan operasi (klausul 8) ISO/IEC 42001, termasuk pengelolaan sumber daya AI, kompetensi, kesadaran, komunikasi, informasi terdokumentasi, pengadaan AI, pengelolaan pihak ketiga, pengawasan manusia, serta pengendalian perubahan sistem AI.

A. Resources

Klausul 7.1 mewajibkan organisasi untuk menentukan dan menyediakan sumber daya yang diperlukan untuk AIMS. Pada sistem AI, sumber daya tidak hanya berupa anggaran dan personel, tetapi juga data, perangkat lunak, infrastruktur komputasi, dan keahlian khusus. Kontrol A.4 menjabarkan kebutuhan tersebut ke dalam lima kontrol, yaitu dokumentasi sumber daya (A.4.2), sumber daya data (A.4.3), sumber daya perkakas (A.4.4), sumber daya sistem dan komputasi (A.4.5), serta sumber daya manusia (A.4.6).

Tabel 5. 1: Jenis Sumber Daya Sistem AI Menurut Kontrol A.4

Sumber Daya	Hal yang Didokumentasikan	Contoh Bukti
Data (A.4.3)	Asal data, kategori, kualitas, retensi, hak penggunaan	Katalog data, <i>datasheet</i> dataset
Perkakas (A.4.4)	<i>Framework</i> ML, pustaka, <i>platform</i> MLOps, alat pelabelan dan evaluasi	Daftar <i>software bill of materials</i> (SBOM) AI
Sistem dan komputasi (A.4.5)	GPU/CPU, <i>cloud</i> , <i>edge</i> , kapasitas penyimpanan dan jaringan	Arsitektur infrastruktur, kontrak <i>cloud</i>
Manusia (A.4.6)	Peran, keahlian, dan jumlah personel yang dibutuhkan	Struktur tim, matriks kompetensi

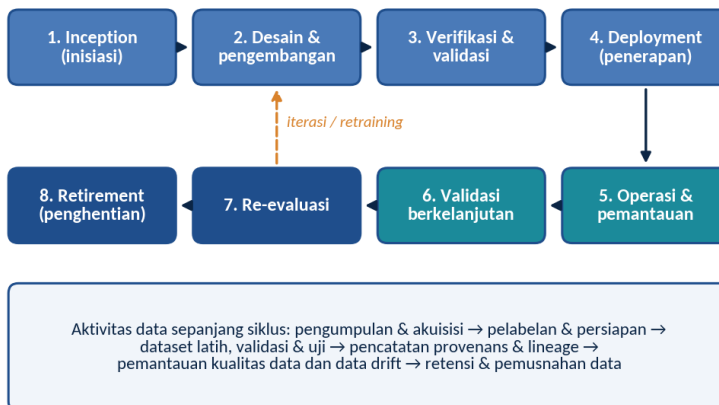
BAB 6

SIKLUS HIDUP SISTEM AI DAN DATA GOVERNANCE

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu menjelaskan tahapan siklus hidup sistem AI menurut ISO/IEC 22989, menerapkan kontrol A.6 dan A.7 ISO/IEC 42001 pada setiap tahap, mengelola dataset latih, validasi, dan uji, memantau model drift dan data drift, serta menjaga kualitas dan lineage data.

A. AI System Lifecycle

ISO/IEC 22989:2022 menggambarkan siklus hidup sistem AI sebagai rangkaian tahap yang dimulai dari inisiasi (*inception*), desain dan pengembangan, verifikasi dan validasi, *deployment*, operasi dan pemantauan, validasi berkelanjutan, evaluasi ulang (*re-evaluation*), hingga penghentian (*retirement*). Tahapan tersebut tidak selalu linear; sistem berbasis ML sering kembali ke tahap pengembangan melalui pelatihan ulang ketika kinerja menurun atau data berubah. ISO/IEC 5338:2023 melengkapi model ini dengan uraian proses siklus hidup yang lebih rinci.



Gambar 6. 1: Siklus Hidup Sistem AI dan Aktivitas Data

Sumber: Diolah Penulis

BAB 7

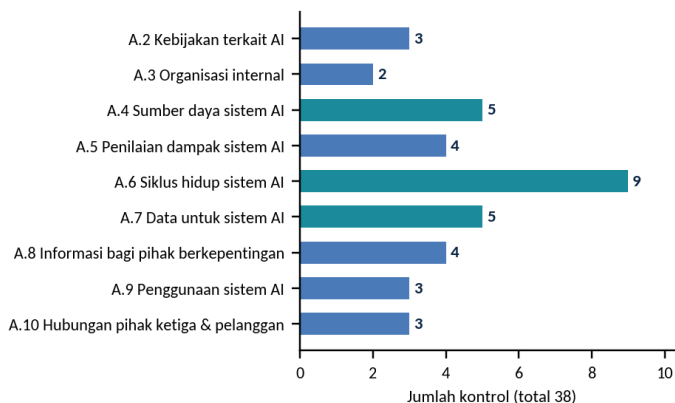
ANNEX A CONTROLS

ISO/IEC 42001

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu menjelaskan sembilan area sasaran kontrol dan 38 kontrol Annex A ISO/IEC 42001, menerapkan kontrol sesuai konteks organisasi, memilih kontrol berdasarkan hasil penilaian risiko, menyiapkan bukti efektivitas kontrol, serta menyusun matriks kontrol AIMS.

A. Konsep Pengendalian AIMS

Annex A ISO/IEC 42001 bersifat normatif dan berisi sasaran kontrol serta kontrol acuan untuk memenuhi sasaran organisasi dan menangani risiko terkait desain dan penggunaan sistem AI. Setiap area diawali dengan sasaran kontrol, lalu diikuti kontrol yang relevan. Annex B memberikan panduan implementasi untuk setiap kontrol. Penting dipahami bahwa organisasi tidak diwajibkan menerapkan seluruh kontrol; kontrol dipilih melalui proses perlakuan risiko dan dijustifikasi dalam SoA. Sebaliknya, Annex A juga tidak lengkap sehingga organisasi dapat menambahkan kontrol lain bila diperlukan.



Gambar 7. 1: Jumlah Kontrol per Area Annex A ISO/IEC 42001

Sumber: Diolah Penulis

BAB 8

AI SYSTEM IMPACT ASSESSMENT, ETIKA, DAN RESPONSIBLE AI

***Tujuan pembelajaran:** Setelah mempelajari bab ini, pembaca diharapkan mampu merancang dan melaksanakan penilaian dampak sistem AI (AIIA) berdasarkan ISO/IEC 42001 dan ISO/IEC 42005, menganalisis dampak terhadap individu dan masyarakat, serta mengelola isu etika seperti bias, halusinasi, bias otomatisasi, keadilan, transparansi, keterjelasan, dan akuntabilitas.*

A. Konsep AI System Impact Assessment

Penilaian dampak sistem AI (*AI System Impact Assessment/AIIA*) adalah proses untuk mengidentifikasi, mengevaluasi, dan menangani konsekuensi potensial pengembangan, penyediaan, atau penggunaan sistem AI terhadap individu, kelompok individu, dan masyarakat. Klausul 6.1.4 ISO/IEC 42001 mewajibkan organisasi menetapkan proses AIIA yang mempertimbangkan *deployment*, tujuan penggunaan, dan penyalahgunaan yang dapat diperkirakan, dengan memperhatikan konteks teknis, sosial, dan yurisdiksi. Hasil AIIA harus didokumentasikan dan dipertimbangkan dalam penilaian risiko.

ISO/IEC 42005:2025 memberikan panduan rinci tentang cara membangun proses AIIA dan mendokumentasikan hasilnya. Standar ini memosisikan AIIA sebagai bagian dari ekosistem tata kelola, risiko, dan penilaian kesesuaian bersama ISO/IEC 38507, ISO/IEC 23894, dan ISO/IEC 42001. Klausul 5 ISO/IEC 42005 menguraikan pengembangan dan penerapan proses AIIA, sedangkan klausul 6 menguraikan komponen dokumentasi penilaian.

BAB 9

AI DALAM KEAMANAN

INFORMASI DAN KEAMANAN

SIBER

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu menganalisis ancaman dan kerentanan khas sistem AI, seperti prompt injection, jailbreaking, kebocoran informasi sensitif, data poisoning, model extraction, serangan adversarial, risiko rantai pasok, dan shadow AI, serta memahami pemanfaatan AI untuk deteksi ancaman, SOC, deteksi malware dan phishing, dan manajemen kerentanan.

A. AI dan Confidentiality, Integrity, Availability

Prinsip kerahasiaan, integritas, dan ketersediaan (*confidentiality, integrity, availability*/CIA) tetap menjadi landasan keamanan sistem AI. Namun, objek yang dilindungi menjadi lebih luas. Selain aplikasi dan data operasional, organisasi harus melindungi data latih, bobot model, *prompt* sistem, basis pengetahuan RAG, *embedding*, *pipeline* pelatihan, dan log interaksi. Annex C ISO/IEC 42001 menyebut keamanan sebagai sasaran organisasi dan menegaskan bahwa AI, khususnya berbasis ML, memunculkan isu baru seperti *data poisoning*, serangan adversarial, dan pencurian model yang melampaui masalah keamanan informasi klasik.

Tabel 9. 1: Penerapan Prinsip CIA pada Sistem AI

Prinsip	Aset AI yang Dilindungi	Contoh Ancaman
<i>Confidentiality</i>	Data latih, bobot model, <i>prompt</i> sistem, dokumen RAG, log percakapan	Kebocoran data via keluaran model, <i>model extraction</i> , <i>membership inference</i>
<i>Integrity</i>	Dataset, label, model, konfigurasi, keluaran	<i>Data poisoning</i> , <i>backdoor</i> , manipulasi <i>prompt</i> , <i>adversarial example</i>

BAB 10

AIMS, KEAMANAN INFORMASI, DAN PERLINDUNGAN DATA PRIBADI

***Tujuan pembelajaran:** Setelah mempelajari bab ini, pembaca diharapkan mampu mengintegrasikan AIMS dengan ISMS ISO/IEC 27001 dan PIMS ISO/IEC 27701, melakukan penilaian risiko terintegrasi, menerapkan kontrol keamanan pada sistem AI, mengelola insiden AI, serta memenuhi kewajiban perlindungan data pribadi dalam sistem AI sesuai UU Nomor 27 Tahun 2022.*

A. Integrasi AIMS dan ISMS

Banyak organisasi di Indonesia telah menerapkan ISMS berbasis ISO/IEC 27001, baik karena tuntutan pelanggan, regulasi sektor, maupun kebutuhan internal. Annex D ISO/IEC 42001 menyatakan bahwa keamanan merupakan kunci pencapaian sasaran organisasi dengan sistem AI dan bahwa integrasi AIMS dengan ISMS sangat difasilitasi karena keduanya menggunakan struktur yang sama. Integrasi menghindari duplikasi dokumen, audit, dan rapat, sekaligus memastikan risiko AI dan risiko keamanan dibahas dalam satu kerangka.

BAB 11

KEAMANAN *GENERATIVE AI*, LLM, RAG, DAN AI AGENT

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu mengidentifikasi risiko khas *Generative AI*, LLM, RAG, dan AI agent, menerapkan pengamanan prompt, basis data vektor, API, dan AI gateway, menetapkan aturan penggunaan AI publik untuk data perusahaan, serta merancang arsitektur *Generative AI* yang aman.

A. *Generative AI dan Large Language Model*

Generative AI telah mengubah cara organisasi bekerja dalam waktu yang sangat singkat. Asisten penulisan, ringkasan rapat, pembuatan kode, analisis dokumen, dan *chatbot* layanan kini menjadi kasus penggunaan umum. Di balik kemudahan tersebut, *Generative AI* memiliki karakter yang menuntut pengendalian khusus: keluarannya bersifat probabilistik, dapat berbeda untuk masukan yang sama, sulit diuji secara menyeluruh, dan sangat dipengaruhi oleh instruksi dalam bahasa alami.

LLM dibangun di atas arsitektur *Transformer* yang memungkinkan model memperhatikan hubungan antarkata dalam konteks panjang. Model dilatih dengan korpus teks yang sangat besar, kemudian diselaraskan agar mengikuti instruksi dan menghindari keluaran berbahaya. NIST AI 600-1 tentang profil *Generative AI* mengidentifikasi sejumlah risiko khas, antara lain konfabulasi atau halusinasi, privasi data, keamanan informasi, integritas informasi, bias berbahaya, hak kekayaan intelektual, konfigurasi interaksi manusia-AI, dan integrasi komponen dalam rantai nilai.

Tabel 11. 1: Pola Pemanfaatan *Generative AI* di Organisasi

Pola	Contoh	Risiko Utama
Asisten publik	Karyawan memakai layanan AI konsumen	Kebocoran data, <i>shadow AI</i>

BAB 12

IMPLEMENTASI AIMS

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu melaksanakan gap analysis ISO/IEC 42001, menetapkan ruang lingkup dan inventaris sistem AI, menyusun kebijakan dan dokumen AIMS, menjalankan penilaian risiko dan dampak, menetapkan kontrol dan SoA, menyelenggarakan pelatihan, serta menyusun peta jalan implementasi AIMS 30–60–90 hari.

A. Gap Analysis ISO/IEC 42001

Implementasi AIMS sebaiknya diawali dengan *gap analysis*, yaitu penilaian kondisi saat ini terhadap persyaratan klausul 4–10 dan kontrol Annex A. Tujuannya adalah mengetahui apa yang sudah ada, apa yang perlu diperbaiki, dan apa yang harus dibangun dari awal. Organisasi yang telah memiliki ISMS ISO/IEC 27001 umumnya sudah memenuhi sebagian besar persyaratan sistem manajemen generik, sehingga kesenjangan terbesar biasanya terletak pada inventaris AI, penilaian dampak, kontrol siklus hidup, dan tata kelola data AI.

Tabel 12. 1: Skala Penilaian Tingkat Pemenuhan

Skor	Kategori	Kriteria
0	Tidak ada	Persyaratan belum ditangani sama sekali
1	Awal	Praktik ada secara informal, tidak terdokumentasi
2	Sebagian	Terdokumentasi sebagian, penerapan belum konsisten
3	Terpenuhi	Terdokumentasi, diterapkan, dan terdapat bukti
4	Optimal	Terpenuhi, diukur, dan ditingkatkan secara berkelanjutan

Sumber: Diolah Penulis

Tingkat pemenuhan per klausul atau area kontrol dihitung sebagai persentase skor aktual terhadap skor minimum yang dipersyaratkan untuk sertifikasi, yaitu skor 3.

BAB 13

AUDIT DAN SERTIFIKASI AIMS

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu merancang pemantauan dan pengukuran kinerja AIMS, melaksanakan audit internal dan tinjauan manajemen, menangani ketidaksesuaian dan tindakan korektif, serta memahami proses audit sertifikasi tahap 1, tahap 2, surveilans, dan resertifikasi.

A. Pemantauan, Pengukuran, Analisis, dan Evaluasi

Klausul 9.1 mewajibkan organisasi menentukan apa yang perlu dipantau dan diukur, metode yang digunakan, kapan pemantauan dilakukan, siapa yang melakukan, serta kapan hasilnya dianalisis dan dievaluasi. Hasilnya harus tersedia sebagai informasi terdokumentasi. Pada AIMS, pemantauan tidak hanya mencakup kinerja proses tata kelola, tetapi juga kinerja dan perilaku sistem AI itu sendiri.

Tabel 13. 1: Contoh Objek Pemantauan dan Pengukuran AIMS

Objek	Indikator	Sumber Data
Proses tata kelola	Persentase sistem AI terinventarisasi, AIIA tepat waktu	Register AIMS
Kinerja model	Akurasi, <i>drift</i> , tingkat halusinasi	Dasbor MLOps
Keadilan	Rasio <i>disparate impact</i> , keluhan diskriminasi	Uji <i>fairness</i> , kanal keluhan
Keamanan	Percobaan <i>prompt injection</i> , pelanggaran DLP	AI <i>gateway</i> , SIEM
Kepatuhan penggunaan	Temuan <i>shadow AI</i> , pelanggaran AUP	<i>Proxy</i> , CASB
Kompetensi	Persentase personel terlatih	Sistem pembelajaran
Pemasok	Persentase pemasok AI dinilai	Register pemasok

Sumber: Diolah Penulis

Analisis hasil pemantauan sebaiknya melihat tren, bukan hanya nilai sesaat. Kenaikan bertahap tingkat *override* manusia atau keluhan

BAB 14

STUDI KASUS PENERAPAN AIMS

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu menerapkan konsep AIMS pada kasus nyata di bidang keamanan siber, perlindungan data pribadi, dan sektor industri, dengan mengidentifikasi risiko, dampak, kontrol ISO/IEC 42001 yang relevan, serta bukti implementasinya.

A. AI untuk Security Operations Center

Sebuah perusahaan penyedia layanan keamanan terkelola menerapkan model ML untuk memprioritaskan *alert* dari SIEM dan LLM untuk meringkas insiden bagi analis L1. Dalam tiga bulan, waktu triase berkurang secara signifikan. Namun, audit internal menemukan bahwa model prioritisasi tidak pernah divalidasi ulang sejak dirilis, dan beberapa *alert* serangan kredensial diberi prioritas rendah karena pola serangan berubah.

Studi kasus ini dan seluruh studi kasus berikutnya bersifat ilustratif, disusun dari pola permasalahan yang umum ditemui dalam praktik, dan tidak merujuk pada organisasi tertentu.

Tabel 14. 1: Studi Kasus AI pada SOC

Aspek	Risiko / Dampak	Penerapan AIMS dan Bukti
Kinerja model	<i>False negative</i> akibat <i>drift</i> taktik penyerang	Pemantauan <i>recall</i> bulanan, validasi ulang triwulanan (A.6.2.6)
Halusinasi ringkasan	Analisis salah memahami insiden	Ringkasan wajib menautkan <i>alert</i> asli; verifikasi analisis (A.9.2)
Bias otomatisasi	Analisis mengabaikan <i>alert</i> berprioritas rendah	Sampling acak <i>alert</i> rendah untuk ditinjau manual
Inventaris	Model SOC tidak tercatat sebagai sistem AI	Dimasukkan ke inventaris dan <i>risk register</i> AIMS

Sumber: Diolah Penulis

BAB 15

KESIMPULAN, MODEL KEMATANGAN, DAN REKOMENDASI

Tujuan pembelajaran: Setelah mempelajari bab ini, pembaca diharapkan mampu merangkum konsep utama AIMS, menilai tingkat kematangan AIMS organisasinya, serta menyusun langkah peningkatan berdasarkan rekomendasi yang diberikan.

A. Kesimpulan

Kecerdasan buatan telah menjadi bagian dari proses inti organisasi, mulai dari layanan pelanggan, keputusan kredit, layanan kesehatan, hingga operasi keamanan siber. Buku ini menunjukkan bahwa manfaat AI hanya dapat dinikmati secara berkelanjutan apabila risiko dan dampaknya dikelola secara sistematis. ISO/IEC 42001:2023 menyediakan kerangka sistem manajemen yang menerjemahkan prinsip *responsible AI* menjadi kebijakan, proses, kontrol, dan bukti yang dapat diaudit.

Beberapa kesimpulan utama dapat dirumuskan. Pertama, AIMS menuntut organisasi memahami perannya terhadap setiap sistem AI dan mencatat seluruh sistem tersebut dalam inventaris. Kedua, risiko AI harus dinilai terhadap organisasi, individu, dan masyarakat, dengan penilaian dampak sistem AI sebagai masukan penting. Ketiga, 38 kontrol Annex A dipilih berdasarkan risiko dan dijustifikasi dalam SoA. Keempat, keamanan informasi dan perlindungan data pribadi merupakan bagian tak terpisahkan dari AI yang tepercaya, sehingga integrasi AIMS dengan ISMS, PIMS, dan kewajiban UU PDP menjadi pendekatan paling efisien. Kelima, *Generative AI*, RAG, dan *AI agent* memerlukan kontrol khusus seperti *AI gateway*, pengamanan *prompt*, dan pembatasan kewenangan agen.

LAMPIRAN

Lampiran ini memuat *template* dan *checklist* yang dapat langsung disesuaikan oleh organisasi dalam membangun dan menerapkan AIMS. Isian contoh bersifat ilustratif dan perlu disesuaikan dengan konteks, ruang lingkup, dan hasil penilaian risiko masing-masing organisasi.

LAMPIRAN A — *Template AI System Inventory*

Template ini digunakan untuk mencatat setiap sistem AI yang dikembangkan, disediakan, atau digunakan organisasi, termasuk layanan AI pihak ketiga. Satu baris atau satu lembar diisi untuk setiap sistem AI dan diperbarui setiap terjadi perubahan signifikan.

Tabel L.A. 1: *Template Inventaris Sistem AI*

Atribut	Contoh Isian
ID sistem / versi	AI-003 / v2.1
Nama sistem	Asisten Virtual Layanan Nasabah
Unit dan pemilik sistem	Divisi Digital Banking / Kepala Layanan Digital
Tujuan bisnis	Menjawab pertanyaan produk dan status layanan 24 jam
Penggunaan yang dimaksud	Informasi umum produk; tidak untuk keputusan kredit atau keluhan formal
Penggunaan yang dilarang	Memberikan nasihat investasi personal, mengubah data nasabah
Peran organisasi	<i>AI customer</i> (LLM pihak ketiga) dan <i>AI provider</i> (layanan ke nasabah)
Jenis teknologi	LLM + RAG atas basis pengetahuan produk
Pengguna dan pihak terdampak	Nasabah ritel, petugas <i>contact center</i>
Kategori data	Pertanyaan nasabah, nomor rekening (dimasking), dokumen produk
Data pribadi / data spesifik	Ya / Tidak
Pihak ketiga dan lokasi pemrosesan	Penyedia LLM X, wilayah pusat data Y

Atribut	Contoh Isian
Tingkat otomatisasi	Pendukung informasi dengan eskalasi ke petugas (HOTL)
Klasifikasi risiko awal	Sedang
Status AIIA / DPIA	Selesai (AIIA-003, 12-05-2026) / Selesai
Status siklus hidup	Produksi
Tanggal tinjauan berikutnya	November 2026

Sumber: Diolah Penulis

LAMPIRAN B — *Template AI Risk Register*

AI risk register mencatat risiko setiap sistem AI beserta analisis, evaluasi, perlakuan, dan risiko residual. Skor dihitung dengan skala dan rumus pada Bab 4.

Tabel L.B. 1: *Template AI Risk Register*

ID	Sistem AI	Deskripsi Risiko (sebab – kejadian – akibat)	L	I	Skor	Kontrol Rencana / Perlakuan	Skor Sisa	Pemilik / Tenggat
R-01	AI-003 Asisten Virtual	Karena masukan tidak difilter, penyerang menyisipkan instruksi sehingga <i>chatbot</i> memberi informasi keliru kepada nasabah	4	4	16	Filter <i>prompt</i> , <i>red teaming</i> , pembatasan domain (A.6.2.4)	6,4	<i>Product owner</i> / Q3
R-02	AI-001 <i>Credit scoring</i>	Karena data latih tidak representatif, pemohon UMKM ditolak secara tidak adil	3	4	12	Uji <i>fairness</i> , penghapusan fitur <i>proxy</i> , peninjauan manusia (A.5.4)	6,0	Kepala risiko kredit / Q3
R-03								

Sumber: Diolah Penulis

Keterangan:

L = kemungkinan (1–5);

I = nilai tertinggi dari dampak terhadap organisasi, individu, dan masyarakat (1–5);

Skor = $L \times I$;

Skor Sisa = skor setelah memperhitungkan efektivitas kontrol.

LAMPIRAN C — *Template AI System Impact Assessment*

Template AIIA ini mengacu pada komponen dokumentasi ISO/IEC 42005 dan dapat digabungkan dengan DPIA apabila sistem memproses data pribadi.

Tabel L.C. 1: *Template AI System Impact Assessment*

Bagian	Pertanyaan Panduan	Isian
1. Ruang lingkup	Sistem, versi, dan batas penilaian apa yang dinilai? Apa pemicu penilaian ini?	
2. Informasi sistem AI	Apa tujuan, fungsi, penggunaan yang dimaksud, dan penggunaan yang tidak dimaksud?	
3. Informasi data	Apa sumber, kategori, kualitas, dan keterwakilan data? Adakah data pribadi spesifik?	
4. Algoritma dan model	Jenis model, asal model, proses pengembangan, dan batasan yang diketahui?	
5. Lingkungan <i>deployment</i>	Wilayah, bahasa, kanal, dan kendala lingkungan operasi?	
6. Pihak berkepentingan	Siapa yang terdampak langsung? Adakah kelompok rentan?	
7. Manfaat	Manfaat apa yang diharapkan bagi individu, organisasi, dan masyarakat?	
8. Kerugian terhadap individu	Dampak terhadap hak, keadilan, privasi, keselamatan, otonomi?	
9. Kerugian terhadap masyarakat	Dampak sosial, lingkungan, dan terhadap kelompok tertentu?	
10. Kegagalan dan penyalahgunaan	Apa akibat bila sistem gagal atau disalahgunakan secara dapat diperkirakan?	
11. Tingkat dampak	Skala dampak (1–5) dan kategori penggunaan sensitif/terbatas?	
12. Tindakan	Mitigasi, pengawasan manusia, informasi bagi pengguna, penanggung jawab, tenggat?	
13. Persetujuan	Nama, jabatan, tanggal persetujuan, dan jadwal tinjauan ulang?	

Sumber: Diolah Penulis

LAMPIRAN D — *Template AI Policy*

Template berikut memberikan contoh rumusan ringkas kebijakan AI yang dapat disesuaikan dengan bahasa dan struktur kebijakan organisasi.

Tabel L.D. 1: Template Kebijakan Kecerdasan Buatan

Bagian	Contoh Rumusan
Tujuan	Kebijakan ini menetapkan arah dan komitmen organisasi dalam mengembangkan, menyediakan, dan menggunakan sistem AI secara bertanggung jawab, aman, dan patuh hukum.
Ruang lingkup	Berlaku bagi seluruh unit, karyawan, dan pihak ketiga yang mengembangkan, menyediakan, atau menggunakan sistem AI atas nama organisasi.
Prinsip	Organisasi berkomitmen pada keadilan, transparansi, keamanan, perlindungan data pribadi, akuntabilitas, pengawasan manusia, dan keberlanjutan.
Komitmen	Memenuhi peraturan yang berlaku termasuk UU PDP; menilai risiko dan dampak sebelum sistem AI digunakan; meningkatkan AIMS secara berkelanjutan.
Penggunaan yang dilarang	Keputusan final berdampak hukum tanpa peninjauan manusia; memasukkan data rahasia ke layanan AI tidak resmi; penggunaan AI untuk manipulasi atau diskriminasi.
Peran	Direksi menetapkan arah; komite tata kelola AI mengawasi; pemilik sistem bertanggung jawab atas risiko sistemnya; CISO dan DPO memberikan pengawasan keamanan dan privasi.
Pelaporan	Setiap karyawan wajib melaporkan kekhawatiran terkait AI melalui kanal resmi tanpa risiko pembalasan.
Kepatuhan	Pelanggaran kebijakan ditangani sesuai ketentuan disiplin organisasi.
Tinjauan	Kebijakan ditinjau minimal setahun sekali atau saat terjadi perubahan signifikan.

Sumber: Diolah Penulis

LAMPIRAN E — *Template AIMS Control Matrix*

Matriks ini mencantumkan seluruh 38 kontrol Annex A ISO/IEC 42001 dengan kolom yang dapat diisi oleh organisasi. Judul kontrol merupakan terjemahan penulis; rujuk teks resmi standar untuk rumusan persyaratan.

Tabel L.E. 1: Template AIMS Control Matrix

Kontrol	Topik	Berlaku (Y/T)	Pemilik	Bukti yang Diharapkan	Status	Efektif
A.2.2	Kebijakan AI			Kebijakan AI disahkan		
A.2.3	Keselarasan dengan kebijakan lain			Pemetaan kebijakan		
A.2.4	Tinjauan kebijakan AI			Notulen tinjauan		
A.3.2	Peran dan tanggung jawab AI			SK, RACI		
A.3.3	Pelaporan kekhawatiran			Prosedur dan rekaman laporan		
A.4.2	Dokumentasi sumber daya			Register sumber daya		
A.4.3	Sumber daya data			Katalog data		
A.4.4	Sumber daya perkakas			Daftar perkakas/SBOM AI		
A.4.5	Sumber daya sistem dan komputasi			Arsitektur infrastruktur		
A.4.6	Sumber daya manusia			Matriks kompetensi		
A.5.2	Proses penilaian dampak sistem AI			Prosedur AIIA		
A.5.3	Dokumentasi penilaian dampak			Laporan AIIA		

Kontrol	Topik	Berlaku (Y/T)	Pemilik	Bukti yang Diharapkan	Status	Efektif
A.5.4	Dampak terhadap individu/ kelompok			Analisis dampak individu		
A.5.5	Dampak sosial			Analisis dampak sosial		
A.6.1.2	Sasaran pengembangan bertanggung jawab			Sasaran dalam persyaratan proyek		
A.6.1.3	Proses desain & pengembangan bertanggung jawab			Prosedur SDLC/MLOps		
A.6.2.2	Persyaratan dan spesifikasi			Dokumen persyaratan		
A.6.2.3	Dokumentasi desain dan pengembangan			Dokumen desain		
A.6.2.4	Verifikasi dan validasi			Laporan pengujian		
A.6.2.5	<i>Deployment</i>			Rencana dan persetujuan rilis		
A.6.2.6	Operasi dan pemantauan			Dasbor, tiket perbaikan		
A.6.2.7	Dokumentasi teknis			<i>Model card</i> , manual		
A.6.2.8	Pencatatan log kejadian			Konfigurasi dan sampel log		
A.7.2	Data untuk pengembangan dan peningkatan			Prosedur data AI		
A.7.3	Perolehan data			Catatan sumber dan lisensi		
A.7.4	Kualitas data			Profil kualitas data		
A.7.5	Provenans data			Catatan <i>lineage</i>		
A.7.6	Persiapan data			Kriteria persiapan data		

Kontrol	Topik	Berlaku (Y/T)	Pemilik	Bukti yang Diharapkan	Status	Efektif
A.8.2	Dokumentasi dan informasi bagi pengguna			Pemberitahuan AI, panduan		
A.8.3	Pelaporan eksternal			Kanal pelaporan dampak		
A.8.4	Komunikasi insiden			Rencana komunikasi insiden		
A.8.5	Informasi bagi pihak berkepentingan			Register kewajiban pelaporan		
A.9.2	Proses penggunaan bertanggung jawab			AUP GenAI, prosedur		
A.9.3	Sasaran penggunaan bertanggung jawab			Sasaran penggunaan		
A.9.4	Penggunaan sesuai tujuan			Pemantauan penggunaan		
A.10.2	Alokasi tanggung jawab			Matriks tanggung jawab bersama		
A.10.3	Pemasok			Penilaian pemasok, kontrak		
A.10.4	Pelanggan			Informasi dan kesepakatan pelanggan		

Sumber: Diolah Penulis

LAMPIRAN F — *Template Generative AI Acceptable Use Policy*

Kebijakan penggunaan *Generative AI* (AUP GenAI) mengatur perilaku karyawan dalam menggunakan layanan AI generatif dan menjadi bukti utama kontrol A.9.2.

Tabel L.F. 1: *Template AUP Generative AI*

Ketentuan	Contoh Rumusan
Alat yang diizinkan	Karyawan hanya menggunakan layanan AI yang tercantum dalam daftar alat AI resmi organisasi.
Data yang dilarang	Dilarang memasukkan data rahasia, data pribadi pelanggan atau karyawan, kode sumber inti, kredensial, dan dokumen klien ke layanan AI yang tidak disetujui untuk klasifikasi tersebut.
Verifikasi keluaran	Pengguna bertanggung jawab memeriksa kebenaran, kelengkapan, dan kepatutan keluaran AI sebelum digunakan.
Keputusan	Keluaran AI tidak boleh menjadi satu-satunya dasar keputusan yang berdampak pada hak, keuangan, atau keselamatan individu.
Pengungkapan	Dokumen eksternal atau materi resmi yang dibuat dengan bantuan AI signifikan wajib ditinjau atasan dan, bila diwajibkan, diberi keterangan.
Hak kekayaan intelektual	Pengguna menghindari pembuatan konten yang meniru karya pihak lain dan mematuhi ketentuan lisensi layanan AI.
Alat baru	Permintaan penggunaan alat AI baru diajukan melalui proses persetujuan yang melibatkan TI, keamanan, dan privasi.
Pelaporan	Kebocoran data atau keluaran berbahaya dilaporkan segera ke kanal insiden.
Pemantauan	Organisasi dapat memantau penggunaan layanan AI pada perangkat dan jaringan kerja sesuai ketentuan yang berlaku.
Sanksi	Pelanggaran ditangani sesuai peraturan disiplin dan kebijakan keamanan informasi.

Sumber: Diolah Penulis

LAMPIRAN G — Checklist Gap Analysis ISO/IEC 42001

Checklist ini digunakan pada tahap awal implementasi. Setiap butir dinilai dengan skala 0–4 sebagaimana dijelaskan pada Bab 12.

Tabel L.G. 1: Checklist Gap Analysis ISO/IEC 42001

Klausul	Pertanyaan	Skor	Bukti
4.1	Isu internal/eksternal dan peran organisasi terhadap AI telah ditentukan?		
4.2	Pihak berkepentingan dan persyaratannya telah diidentifikasi?		
4.3	Ruang lingkup AIMS terdokumentasi?		
5.1	Manajemen puncak menunjukkan komitmen dan menyediakan sumber daya?		
5.2	Kebijakan AI ditetapkan, dikomunikasikan, dan tersedia?		
5.3	Peran, tanggung jawab, dan wewenang AIMS ditetapkan?		
6.1.1	Kriteria risiko AI dan kriteria penerimaan ditetapkan?		
6.1.2	Proses penilaian risiko AI terdokumentasi dan konsisten?		
6.1.3	Proses perlakuan risiko, SoA, dan rencana perlakuan tersedia?		
6.1.4	Proses AIIA ditetapkan dan hasilnya dipakai dalam penilaian risiko?		
6.2	Sasaran AI terukur dan direncanakan pencapaiannya?		
6.3	Perubahan AIMS direncanakan?		
7.1–7.3	Sumber daya, kompetensi, dan kesadaran terpenuhi?		
7.4–7.5	Komunikasi dan informasi terdokumentasi dikendalikan?		
8.1	Proses operasional dan pihak eksternal dikendalikan?		
8.2–8.4	Penilaian risiko, perlakuan, dan AIIA dilaksanakan secara berkala?		

Klausul	Pertanyaan	Skor	Bukti
9.1	Pemantauan dan pengukuran kinerja AIMS dilakukan?		
9.2	Program audit internal dijalankan?		
9.3	Tinjauan manajemen dilaksanakan?		
10.1– 10.2	Peningkatan dan tindakan korektif berjalan?		
Annex A	Apakah seluruh 38 kontrol telah dinilai dan dijustifikasi dalam SoA?		

Sumber: Diolah Penulis

LAMPIRAN H — Checklist Internal Audit AIMS

Checklist ini membantu auditor internal menguji penerapan AIMS pada sampel sistem AI. Auditor mencatat bukti yang diperiksa dan kesimpulan kesesuaian.

Tabel L.H. 1: Checklist Internal Audit AIMS

Rujukan	Pertanyaan Audit	Bukti yang Diperiksa	Hasil (S/KS)
4.3	Apakah sistem AI sampel tercakup dalam ruang lingkup dan inventaris?	Inventaris, ruang lingkup	
5.2	Apakah pengguna sampel mengetahui kebijakan AI dan AUP?	Wawancara, catatan pelatihan	
6.1.2	Apakah risiko sistem sampel dinilai dengan metodologi yang berlaku?	<i>Risk register</i>	
6.1.4	Apakah AIIA dilakukan sebelum <i>go-live</i> dan disetujui?	Laporan AIIA	
6.1.3	Apakah kontrol pada SoA diterapkan untuk sistem sampel?	SoA, bukti kontrol	
A.6.2.4	Apakah laporan verifikasi dan validasi disetujui sebelum rilis?	Laporan uji, tiket rilis	
A.6.2.6	Apakah kinerja dan <i>drift</i> model dipantau sesuai ambang?	Dasbor, tiket tindak lanjut	
A.6.2.8	Apakah log kejadian tersedia dan dilindungi?	Sampel log	
A.7.3–A.7.5	Apakah sumber, kualitas, dan provenans data terdokumentasi?	Katalog data, <i>lineage</i>	
A.8.2	Apakah pengguna diberi informasi bahwa mereka berinteraksi dengan AI?	Tampilan antarmuka	
A.9.2	Apakah penggunaan GenAI tidak sah terdeteksi dan ditindaklanjuti?	Log DLP/CASB	
A.10.3	Apakah penyedia AI dinilai dan kontraknya memuat klausul penggunaan data?	Penilaian pemasok, kontrak	

Rujukan	Pertanyaan Audit	Bukti yang Diperiksa	Hasil (S/KS)
7.2	Apakah personel kunci memiliki bukti kompetensi?	Sertifikat, matriks kompetensi	
9.1	Apakah KPI/KRI AIMS dilaporkan dan dianalisis?	Laporan kinerja	
10.2	Apakah ketidaksesuaian sebelumnya ditutup dan diverifikasi?	Register tindakan korektif	

Sumber: Diolah Penulis

Keterangan:

S = sesuai;

KS = tidak sesuai (diklasifikasikan sebagai mayor atau minor).

LAMPIRAN I — *Template Privacy Impact Assessment*

Template PIA/DPIA ini disusun berdasarkan kewajiban Pasal 34 UU PDP dan pedoman ISO/IEC 29134, disesuaikan untuk pemrosesan data pribadi oleh sistem AI.

Tabel L.I. 1: *Template Privacy Impact Assessment* untuk Sistem AI

Bagian	Pertanyaan Panduan	Isian
Deskripsi pemrosesan	Tujuan, sistem AI, jenis data pribadi, subjek data, dan volume?	
Kriteria risiko tinggi	Keputusan otomatis, data spesifik, skala besar, pemprofilan, teknologi baru?	
Dasar pemrosesan	Dasar pemrosesan yang sah menurut Pasal 20 UU PDP?	
Kebutuhan dan proporsionalitas	Apakah data minimum? Adakah alternatif yang lebih sedikit mengganggu privasi?	
Aliran data	Dari mana data diperoleh, ke mana dikirim, termasuk penyedia model dan transfer luar negeri?	
Hak subjek data	Bagaimana hak akses, koreksi, penghapusan, dan keberatan atas keputusan otomatis dipenuhi?	
Risiko privasi	Kebocoran, inferensi sensitif, penggunaan di luar tujuan, retensi berlebihan?	
Kontrol	Pseudonimisasi, enkripsi, kontrol akses, PET, masking log, kontrak pemrosesan?	
Risiko residual	Tingkat risiko setelah kontrol dan keputusan penerimaan?	
Konsultasi	Pendapat DPO dan pihak terkait?	
Persetujuan	Nama, jabatan, tanggal, dan jadwal tinjauan ulang?	

Sumber: Diolah Penulis

LAMPIRAN J — Mapping AIMS-ISMS-Privacy

Pemetaan ini membantu organisasi mengintegrasikan kontrol AIMS dengan kontrol ISMS ISO/IEC 27001/27002 dan kewajiban privasi. Nomor kontrol ISO/IEC 27002 merujuk pada edisi 2022; kewajiban privasi merujuk pada UU PDP dan tema ISO/IEC 27701.

Tabel L.J. 1: Pemetaan AIMS, ISMS, dan Privasi

Tema	ISO/IEC 42001	ISO/IEC 27001/27002:2022	Privasi (UU PDP / ISO/IEC 27701)
Kebijakan	5.2, A.2	5.2, 5.1	Kebijakan perlindungan data pribadi
Peran & tanggung jawab	5.3, A.3.2	5.3, 5.2	Pejabat/petugas PDP (Pasal 53)
Risiko	6.1.2, 6.1.3	6.1.2, 6.1.3	Penilaian risiko privasi
Penilaian dampak	6.1.4, A.5	—	DPIA (Pasal 34)
Inventaris aset	A.4.2–A.4.5	5.9	Register aktivitas pemrosesan
Data	A.7.2–A.7.6	5.12, 5.33, 8.10	Prinsip pemrosesan (Pasal 16), dasar pemrosesan (Pasal 20)
Pengembangan aman	A.6.1.3, A.6.2.4	8.25, 8.28, 8.29	<i>Privacy by design</i>
Log & pemantauan	A.6.2.6, A.6.2.8	8.15, 8.16	Minimisasi dan masking log
Kontrol akses	A.6.2.5	5.15, 8.2, 8.3, 8.5	Pembatasan akses data pribadi
Pemasok	A.10.2, A.10.3	5.19–5.23	Kontrak dengan prosesor data, transfer (Pasal 56)
Insiden	A.8.4	5.24–5.28	Notifikasi 3 × 24 jam (Pasal 46)

Tema	ISO/IEC 42001	ISO/IEC 27001/27002:2022	Privasi (UU PDP / ISO/IEC 27701)
Informasi bagi pengguna	A.8.2, A.8.5	—	Transparansi pemrosesan, hak subjek data
Keputusan otomatis	A.9.2, A.9.3	—	Hak keberatan (Pasal 10)
Audit & tinjauan	9.2, 9.3	9.2, 9.3	Audit kepatuhan PDP

Sumber: Diolah Penulis

DAFTAR SINGKATAN

Singkatan	Kepanjangan / Keterangan
AI	<i>Artificial intelligence</i> (kecerdasan buatan)
AIIA	AI System Impact Assessment (penilaian dampak sistem AI)
AIMS	<i>Artificial intelligence</i> Management System (sistem manajemen kecerdasan buatan)
API	Application Programming Interface
AUC	Area Under the Curve
AUP	Acceptable Use Policy (kebijakan penggunaan yang dapat diterima)
CASB	Cloud Access Security Broker
CI/CD	Continuous Integration / Continuous Delivery
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
DI	Disparate Impact
DLP	Data Loss Prevention
DPIA	Data Protection Impact Assessment (penilaian dampak perlindungan data pribadi)
DPO	Data Protection Officer (pejabat/petugas perlindungan data pribadi)
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
ERM	Enterprise Risk Management
EU AI Act	Regulation (EU) 2024/1689 tentang Kecerdasan Buatan
FGSM	Fast Gradient Sign Method
FN	False Negative
FP	False Positive
GenAI	<i>Generative Artificial intelligence</i>
GPU	Graphics Processing Unit

Singkatan	Kepanjangan / Keterangan
HIC	Human-in-Command
HITL	Human-in-the-Loop
HOTL	Human-on-the-Loop
IAM	Identity and Access Management
IEC	International Electrotechnical Commission
ISMS	Information Security Management System (sistem manajemen keamanan informasi)
ISO	International Organization for Standardization
JTC	Joint Technical Committee
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LIME	Local Interpretable Model-agnostic Explanations
LLM	Large Language Model
ML	<i>Machine learning</i>
MLOps	<i>Machine learning</i> Operations
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
OECD	Organisation for Economic Co-operation and Development
OJK	Otoritas Jasa Keuangan
OWASP	Open Worldwide Application Security Project
PDCA	Plan-Do-Check-Act
PDP	Pelindungan Data Pribadi
PET	Privacy-Enhancing Technologies
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIMS	Privacy Information Management System (sistem manajemen informasi privasi)
PSI	Population Stability Index
RACI	Responsible, Accountable, Consulted, Informed
RAG	Retrieval-Augmented Generation

Singkatan	Kepanjangan / Keterangan
SaaS	Software as a Service
SBOM	Software Bill of Materials
SC 42	Subcommittee 42 <i>Artificial intelligence</i> ISO/IEC JTC 1
SDLC	Software Development Life Cycle
SE	Surat Edaran
SHAP	SHapley Additive exPlanations
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SoA	Statement of Applicability (pernyataan keberlakuan)
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
TP	True Positive
TPR	True Positive Rate
UEBA	User and Entity Behavior Analytics
UMKM	Usaha Mikro, Kecil, dan Menengah
UNESCO	United Nations Educational, Scientific and Cultural Organization
UU	Undang-Undang

DAFTAR PUSTAKA

- Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial *machine learning*. *Pattern Recognition*, 84, 317–331. <https://doi.org/10.1016/j.patcog.2018.07.023>
- Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T., Song, D., Erlingsson, Ú., Oprea, A., & Raffel, C. (2021). Extracting training data from large language models. In *Proceedings of the 30th USENIX Security Symposium* (pp. 2633–2650). USENIX Association.
- Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.
- European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on *artificial intelligence* (*Artificial intelligence Act*). *Official Journal of the European Union*, L series.
- European Union Agency for Cybersecurity. (2023). *Multilayer framework for good cybersecurity practices for AI*. ENISA.
- Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM*, 64(12), 86–92. <https://doi.org/10.1145/3458723>
- Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. In *3rd International Conference on Learning Representations (ICLR 2015)*. arXiv:1412.6572.
- Greshake, K., Abdelnabi, S., Mishra, S., Endres, C., Holz, T., & Fritz, M. (2023). Not what you've signed up for: Compromising real-world LLM-integrated applications with indirect prompt injection. In *Proceedings of the 16th ACM Workshop on Artificial intelligence and Security* (pp. 79–90). ACM. <https://doi.org/10.1145/3605764.3623985>
- IBM. (2024). *Cost of a data breach report 2024*. IBM Corporation.

- International Organization for Standardization & International Electrotechnical Commission. (2015). *ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2020). *ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence*. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2021). *ISO/IEC TR 24027:2021 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making*. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2022a). *ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2022b). *ISO/IEC 23053:2022 Framework for artificial intelligence (AI) systems using machine learning (ML)*. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2022c). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2022d). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2022e). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. ISO.
- International Organization for Standardization & International Electrotechnical Commission. (2022f). *ISO/IEC 38507:2022*

Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations. ISO.

International Organization for Standardization & International Electrotechnical Commission. (2023a). *ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management.* ISO.

International Organization for Standardization & International Electrotechnical Commission. (2023b). *ISO/IEC 29134:2023 Information technology — Security techniques — Guidelines for privacy impact assessment.* ISO.

International Organization for Standardization & International Electrotechnical Commission. (2023c). *ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system.* ISO.

International Organization for Standardization & International Electrotechnical Commission. (2023d). *ISO/IEC 5338:2023 Information technology — Artificial intelligence — AI system life cycle processes.* ISO.

International Organization for Standardization & International Electrotechnical Commission. (2024). *ISO/IEC 5259-1:2024 Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology, and examples.* ISO.

International Organization for Standardization & International Electrotechnical Commission. (2025a). *ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance.* ISO.

International Organization for Standardization & International Electrotechnical Commission. (2025b). *ISO/IEC 42005:2025 Information technology — Artificial intelligence (AI) — AI system impact assessment.* ISO.

International Organization for Standardization & International Electrotechnical Commission. (2025c). *ISO/IEC 42006:2025 Information technology — Artificial intelligence — Requirements for*

bodies providing audit and certification of artificial intelligence management systems. ISO.

International Organization for Standardization. (2018a). *ISO 19011:2018 Guidelines for auditing management systems.* ISO.

International Organization for Standardization. (2018b). *ISO 31000:2018 Risk management — Guidelines.* ISO.

Ji, Z., Lee, N., Frieske, R., Yu, T., Su, D., Xu, Y., Ishii, E., Bang, Y. J., Madotto, A., & Fung, P. (2023). Survey of hallucination in natural language generation. *ACM Computing Surveys*, 55(12), 1–38. <https://doi.org/10.1145/3571730>

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial.* Kemenkominfo.

Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., Küttler, H., Lewis, M., Yih, W., Rocktäschel, T., Riedel, S., & Kiela, D. (2020). Retrieval-augmented generation for knowledge-intensive NLP tasks. *Advances in Neural Information Processing Systems*, 33, 9459–9474.

Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. *Advances in Neural Information Processing Systems*, 30, 4765–4774.

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in *machine learning*. *ACM Computing Surveys*, 54(6), 1–35. <https://doi.org/10.1145/3457607>

Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. In *Proceedings of the Conference on Fairness, Accountability, and Transparency* (pp. 220–229). ACM. <https://doi.org/10.1145/3287560.3287596>

MITRE Corporation. (t.t.). *MITRE ATLAS: Adversarial threat landscape for artificial-intelligence systems.* <https://atlas.mitre.org>

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.100-1>

- National Institute of Standards and Technology. (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile* (NIST AI 600-1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.600-1>
- Organisation for Economic Co-operation and Development. (2024). *Recommendation of the Council on Artificial intelligence* (OECD/LEGAL/0449). OECD.
- Otoritas Jasa Keuangan. (2023). *Panduan kode etik kecerdasan artifisial (AI) yang bertanggung jawab dan terpercaya di industri teknologi finansial*. OJK.
- OWASP Foundation. (2024). *OWASP top 10 for LLM applications 2025*. OWASP GenAI Security Project.
- Parasuraman, R., & Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. *Human Factors*, 52(3), 381–410. <https://doi.org/10.1177/0018720810376055>
- Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 33–44). ACM. <https://doi.org/10.1145/3351095.3372873>
- Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185.
- Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
- Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144). ACM. <https://doi.org/10.1145/2939672.2939778>
- Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against *machine learning* models. In *2017 IEEE*

- Symposium on Security and Privacy* (pp. 3–18). IEEE.
<https://doi.org/10.1109/SP.2017.41>
- Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., & Ristenpart, T. (2016). Stealing *machine learning* models via prediction APIs. In *Proceedings of the 25th USENIX Security Symposium* (pp. 601–618). USENIX Association.
- UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. United Nations Educational, Scientific and Cultural Organization.
- Vassilev, A., Oprea, A., Fordyce, A., & Anderson, H. (2024). *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations* (NIST AI 100-2 E2023). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.100-2e2023>
- Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, 30, 5998–6008.

GLOSARIUM

A

Adversarial example

Masukan yang dimodifikasi secara halus, sering tidak disadari manusia, agar model AI menghasilkan keluaran yang salah.

AI agent

Sistem berbasis AI, umumnya LLM, yang mampu merencanakan langkah, memanggil alat atau API, dan bertindak untuk mencapai tujuan yang diberikan.

AI gateway

Lapisan perantara antara pengguna atau aplikasi dan layanan model AI yang menegakkan autentikasi, filter, DLP, kuota, dan pencatatan.

AI governance

Sistem pengarahan, pengendalian, dan akuntabilitas atas pengembangan, pengadaan, dan penggunaan AI dalam organisasi.

AI system impact assessment

Proses formal untuk mengidentifikasi, mengevaluasi, dan menangani dampak sistem AI terhadap individu, kelompok, dan masyarakat.

Akuntabilitas

Kondisi ketika keputusan dan tindakan organisasi atau sistem dapat ditelusuri dan dipertanggungjawabkan kepada pihak yang bertanggung jawab.

Annex A

Lampiran normatif ISO/IEC 42001 yang memuat sasaran kontrol dan 38 kontrol acuan untuk sistem manajemen AI.

Automation bias

Kecenderungan manusia untuk terlalu memercayai keluaran sistem otomatis dan mengabaikan informasi atau penilaian lain.

B

Bias

Perbedaan perlakuan sistematis terhadap objek, orang, atau kelompok dibandingkan dengan yang lain, yang dapat menimbulkan ketidakadilan.

D

Data drift

Pergeseran distribusi data masukan pada saat operasi dibandingkan dengan distribusi data latih.

Data lineage

Catatan aliran data dari sumber, melalui transformasi, hingga digunakan sebagai dataset atau fitur model.

Data poisoning

Serangan yang memanipulasi data latih agar model mempelajari perilaku yang diinginkan penyerang.

Deep learning

Bagian dari *machine learning* yang menggunakan jaringan saraf tiruan berlapis banyak untuk mempelajari representasi data yang kompleks.

Differential privacy

Teknik yang menambahkan derau terukur sehingga kontribusi data individu tidak dapat disimpulkan dari hasil analisis atau model.

E

Embedding

Representasi numerik berdimensi tinggi dari teks atau data lain yang digunakan untuk pencarian kemiripan.

Explainability

Kemampuan sistem AI untuk menyatakan faktor penting yang memengaruhi keputusannya dengan cara yang dapat dipahami manusia.

F

Fairness

Sasaran agar sistem AI tidak menghasilkan perlakuan atau dampak yang tidak adil terhadap individu atau kelompok tertentu.

Federated learning

Pendekatan pelatihan model di lokasi data masing-masing tanpa memindahkan data mentah ke satu tempat.

G

Generative AI

Kelas sistem AI yang mampu menghasilkan konten baru seperti teks, gambar, audio, video, atau kode.

H

Halusinasi

Keluaran model generatif yang tampak meyakinkan tetapi tidak sesuai fakta atau tidak didukung sumber.

Human oversight

Mekanisme yang memungkinkan manusia memahami, memantau, dan mengintervensi atau menghentikan sistem AI.

Human-in-the-loop

Model pengawasan ketika setiap keputusan AI harus disetujui manusia sebelum dieksekusi.

Human-on-the-loop

Model pengawasan ketika AI bertindak secara mandiri tetapi dipantau manusia yang dapat mengintervensi.

I

Informasi terdokumentasi

Informasi yang wajib dikendalikan dan dipelihara organisasi beserta media penyimpanannya.

Intended use

Penggunaan sistem AI sesuai tujuan yang ditetapkan oleh penyedia atau organisasi.

J

Jailbreaking

Upaya melewati pembatasan keselamatan model agar menghasilkan keluaran yang seharusnya ditolak.

K

Kebijakan AI

Pernyataan arah dan komitmen manajemen puncak terkait pengembangan, penyediaan, dan penggunaan AI.

Ketidaksesuaian

Tidak terpenuhinya suatu persyaratan standar, organisasi, atau peraturan.

L

Large Language Model

Model bahasa berukuran sangat besar yang dilatih dengan korpus teks masif dan mampu mengikuti instruksi dalam bahasa alami.

M

Machine learning

Proses mengoptimalkan parameter model melalui teknik komputasi sehingga perilaku model mencerminkan data atau pengalaman.

Membership inference

Serangan privasi untuk menebak apakah suatu data individu termasuk dalam data latih model.

Model card

Dokumen ringkas yang menjelaskan tujuan penggunaan, kinerja, batasan, dan pertimbangan etis sebuah model.

Model drift

Penurunan kinerja model akibat perubahan hubungan antara masukan dan keluaran di dunia nyata.

Model extraction

Serangan untuk mereplikasi fungsi model melalui kueri berulang terhadap API.

P

Pihak berkepentingan

Orang atau organisasi yang dapat memengaruhi, dipengaruhi, atau merasa dipengaruhi oleh keputusan atau aktivitas organisasi.

Privacy by design

Pendekatan yang menanamkan perlindungan privasi sejak tahap desain sistem dan sepanjang siklus hidupnya.

Prompt

Instruksi atau masukan yang diberikan kepada model bahasa, termasuk prompt sistem dan masukan pengguna.

Prompt injection

Serangan yang menyisipkan instruksi ke masukan LLM agar model mengabaikan instruksi sistem atau melakukan tindakan tidak diinginkan.

Provenans data

Informasi asal-usul data dan riwayat perubahannya sepanjang siklus hidup data.

Pseudonimisasi

Pemrosesan yang mengganti pengenalan langsung dengan kode sehingga data tidak dapat dikaitkan dengan individu tanpa informasi tambahan.

R

Red teaming

Pengujian dengan meniru perilaku penyerang untuk menemukan kelemahan keamanan dan keselamatan sistem AI.

Responsible AI

Pendekatan pengembangan dan penggunaan AI yang adil, transparan, aman, menghormati privasi, dan akuntabel.

Retrieval-Augmented Generation

Teknik yang menggabungkan pencarian dokumen dengan model generatif agar jawaban didasarkan pada sumber.

Risiko residual

Risiko yang tersisa setelah perlakuan risiko diterapkan.

S

Shadow AI

Penggunaan alat atau layanan AI oleh karyawan tanpa persetujuan dan pengawasan organisasi.

Siklus hidup sistem AI

Rangkaian tahap sistem AI dari inisiasi, desain, verifikasi, deployment, operasi, evaluasi ulang, hingga penghentian.

Sistem AI

Sistem rekayasa yang menghasilkan keluaran seperti konten, prakiraan, rekomendasi, atau keputusan untuk tujuan yang ditetapkan manusia.

Statement of Applicability

Dokumen yang memuat kontrol yang diperlukan beserta justifikasi inklusi dan eksklusinya.

T

Transparansi

Penyampaian informasi yang tepat tentang organisasi dan sistem AI kepada pemangku kepentingan.

V

Vector database

Basis data yang menyimpan embedding dan mendukung pencarian berdasarkan kemiripan, umum digunakan pada RAG.

INDEKS

A

Accountability — 7, 27, 28, 74
Adversarial — 53, 76, 79, 80
AI agent — 4, 5, 98, 99
AI gateway — 35, 64, 79, 100
AI Governance Committee — 25, 26, 28, 34
AI policy — 24, 25, 59, 135
AI risk register — 9, 15, 36, 132
AI system impact assessment — 36, 67, 75, 107
AI system inventory — 104, 106, 110, 128
Annex A — 14, 19, 34, 58
Anonimisasi — 91
Audit internal — 8, 113, 116, 117
Automation bias — 45, 66, 67, 72

B

Bias — 6, 70, 71, 72

C

Checklist — 9, 19, 138, 139
Credit scoring — 5, 16, 30, 33

D

Data drift — 3, 48, 54
Data lineage — 48, 56, 57, 61
Data poisoning — 6, 30, 76, 79
Data pribadi spesifik — 50, 91, 123, 125
Deep learning — 1, 2, 3, 4
Deployment — 15, 17, 30, 53
Differential privacy — 80, 91
DLP — 36, 121, 122, 123
DPIA — 68, 74, 75, 93

E

Enterprise Risk Management — 37, 38
EU AI Act — 12, 21, 130
Explainability — 3, 7, 15, 73

F

Fairness — 7, 15, 36, 72

G

Gap analysis — 104, 105, 110, 138

Generative AI — 9, 95, 121, 137

H

Halusinasi — 71, 75, 89, 95

Human oversight — 5, 28, 44, 46

Human-in-the-loop — 34, 45, 74, 106

I

Informasi terdokumentasi — 8, 13, 42, 46

ISMS — 85, 86, 93, 141

ISO/IEC 22989 — 2, 4, 16, 48

ISO/IEC 23894 — 6, 11, 18, 29

ISO/IEC 27001 — 8, 11, 85, 86

ISO/IEC 27701 — 8, 11, 14, 17

ISO/IEC 42001 — 11, 19, 58, 86

ISO/IEC 42005 — 11, 18, 67, 68

ISO/IEC 42006 — 19, 115, 117, 118

J

Jailbreaking — 96, 101

K

KPI — 15, 22, 36, 38

KRI — 15, 22, 36, 38

L

Large Language Model — 1, 4, 77, 95

M

Machine learning — 1, 2, 3, 79

Management review — 93, 114, 116, 117

MLOps — 37, 39, 40, 46

Model card — 17, 43, 53, 61

Model drift — 6, 37, 40, 54

Model extraction — 6, 76, 79, 80

O

OWASP — 41, 77, 84, 99

P

PDCA — 12, 13, 15

Pemasok — 43, 46, 63, 112

Pengendalian perubahan — 37, 45, 46, 114
Phishing — 3, 82, 83, 120
Privacy by design — 9, 90, 94, 141
Privacy Impact Assessment — 9, 22, 92, 140
Prompt injection — 5, 35, 78, 84
Pseudonimisasi — 91, 140

R

RACI — 27, 28, 59, 74
Red teaming — 35, 40, 53, 64
Responsible AI — 7, 8, 9, 74
Retrieval-Augmented Generation — 4, 76, 95, 97
Risiko residual — 27, 29, 34, 35
Ruang lingkup AIMS — 13, 21, 23, 105

S

Sertifikasi — 19, 40, 115, 116
Shadow AI — 6, 81, 84, 122
Siklus hidup sistem AI — 9, 48, 49, 56
SOC — 5, 82, 84, 119
Statement of Applicability — 38, 63, 107, 110
Surveilans — 19, 112, 116, 117

T

Tindakan korektif — 13, 112, 114, 115
Transparansi — 5, 7, 8, 73

U

UU PDP — 18, 22, 84, 92

V

Vector database — 95, 98

BIOGRAFI PENULIS



Dr. Nungky Awang Chandra, S.Si., M.TI.

Nungky Awang Chandra lahir di Semarang pada tahun 1973. Selain sebagai dosen Teknik Informatika Fakultas Ilmu Komputer Universitas Mercu Buana, penulis berprofesi sebagai auditor sistem manajemen keamanan informasi ISO/IEC 27001, ISO 22301, ISO/IEC 27701, ISO/IEC 20000, dan ISO/IEC 42001 yang teregistrasi di BSSN. Penulis merupakan lulusan Sarjana (S1) Fisika Komputasi Institut Teknologi Bandung pada tahun 1998, kemudian pada tahun 2007 melanjutkan pendidikan Magister Teknologi Informasi Universitas Indonesia dan menyelesaikannya pada tahun 2009. Pada tahun 2022, penulis menyelesaikan studi S3 di Universitas Indonesia dengan disertasi dan publikasi jurnal bereputasi internasional tentang keamanan siber dan manajemen risiko keamanan siber. Selain itu, pada tahun 2023 penulis menyelesaikan studi *postgraduate cyber security* di Massachusetts Institute of Technology (MIT).

Penulis memiliki kepakaran di bidang keamanan siber, pengembangan aplikasi, dan *drone*. Untuk mewujudkan karier sebagai dosen profesional, penulis aktif sebagai peneliti di bidang kepakarannya. Beberapa penelitian yang telah dilakukan didanai oleh pihak internal perguruan tinggi dan juga Kemenristekdikti. Selain meneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara. Korespondensi dengan penulis dapat dilakukan melalui email: nungkyac707@gmail.com.



Siti Maesaroh, S.Kom., M.T.I.

Ketertarikan penulis terhadap ilmu komputer dimulai pada tahun 2010. Hal tersebut membuat penulis memilih untuk menempuh pendidikan tinggi di bidang Sistem Informasi. Dua tahun setelah lulus S1, penulis menyelesaikan studi S2 pada Program Studi Teknik Informatika Program Pascasarjana Universitas Raharja. Penulis memiliki kepakaran di bidang *Web Technology* dan *Data Science*. Untuk mewujudkan karier sebagai dosen profesional, penulis aktif sebagai peneliti di bidang kepakarannya. Beberapa penelitian yang telah dilakukan didanai oleh internal perguruan tinggi dan juga Kemenristekdikti. Selain meneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara, serta mengembangkan solusi perangkat lunak inovatif yang memecahkan tantangan bisnis melalui keterampilan pemrograman dan pengetahuan teknologi terkini. Email penulis: mays41946@gmail.com.



Mohamad Yusuf, S.Kom., M.C.S.

Penulis dilahirkan di Jakarta pada tanggal 7 September 1976. Pendidikan S1 diselesaikan pada tahun 2001 di Universitas Budi Luhur, Jurusan Teknik Informatika. Selanjutnya, penulis menempuh pendidikan S2 di Preston University Islamabad, Pakistan, dan saat ini sedang menyelesaikan S3 di Universiti Malaysia Kelantan dalam bidang *Data Science*. Penulis adalah dosen tetap Universitas Mercu Buana Jakarta. Buku yang telah dihasilkan antara lain Pemrograman Mobile dengan Flutter, Pemrograman Java, Aplikasi Mobile Teori dan Praktik, Teknik 2D/3D Blender untuk Pemula hingga Ahli, Bahasa Pemrograman Python, serta Pembelajaran Mesin dan Kecerdasan Buatan: Teori dan Aplikasi Praktis. Penulis juga telah menulis buku tentang tata kelola teknologi informasi. Penulis dapat dihubungi melalui email: mhd.yusuf@mercubuana.ac.id.



Diva Alifta Chandra, B.Eng., M.Sc.

Diva Alifta Chandra lahir di Purwokerto pada tahun 2001. Ia merupakan auditor sistem manajemen keamanan informasi yang tersertifikasi ISO/IEC 27001 dan ISO/IEC 27701 dari lembaga internasional IRCA (United Kingdom) dan PECB (Canada). Penulis menyelesaikan pendidikan sarjana (S1) di bidang *Biomedical Engineering* dari Universiti Teknologi Malaysia (UTM), kemudian meraih gelar *Master of Data Science* dari University of Malaya (UM) dengan disertasi yang berfokus pada *Algorithmic Social Computing*. Selain berkarier sebagai auditor, penulis aktif berprofesi sebagai *Penetration Tester* dan *SOC Analyst*. Dengan kepakaran di bidang keamanan siber dan ilmu data, penulis berkomitmen untuk mengembangkan karier sebagai dosen dan peneliti profesional, serta aktif meneliti dan menulis artikel ilmiah seputar *social computing*. Untuk korespondensi, penulis dapat dihubungi melalui email: divaac56@gmail.com.

Sistem Manajemen Kecerdasan Buatan (AIMS) ISO/IEC 42001:2023

Kecerdasan buatan kini menjadi tulang punggung layanan digital, pengambilan keputusan bisnis, dan operasi keamanan siber. Namun, di balik manfaatnya, AI membawa risiko baru: kebocoran data melalui Generative AI, prompt injection, bias keputusan, halusinasi, serangan terhadap model, hingga pelanggaran perlindungan data pribadi. Organisasi membutuhkan kerangka tata kelola yang tidak hanya berisi prinsip, tetapi juga dapat diterapkan, diukur, dan diaudit. Buku ini menyajikan panduan praktis membangun Sistem Manajemen Kecerdasan Buatan (Artificial Intelligence Management System/AIMS) berbasis ISO/IEC 42001:2023 standar sistem manajemen AI pertama di dunia yang dapat disertifikasi. Pembahasan dimulai dari konsep dasar AI dan struktur standar, dilanjutkan dengan konteks organisasi dan tata kelola AI, manajemen risiko dan penilaian dampak sistem AI, 38 kontrol Annex A, keamanan LLM, RAG, dan AI agent, integrasi dengan ISO/IEC 27001, ISO/IEC 27701, dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, hingga implementasi, audit, sertifikasi, dan studi kasus lintas sektor. Sebanyak 122 tabel, 23 gambar, checklist evaluasi di setiap bab, serta sepuluh lampiran template siap pakai menjadikan buku ini bukan sekadar bacaan teoretis, melainkan pendamping kerja bagi organisasi yang sedang membangun tata kelola AI.

Keunggulan Buku:

-  Berbasis standar mutakhir. Mengacu langsung pada ISO/IEC 42001:2023, ISO/IEC 22989:2022, ISO/IEC 23894:2023, ISO/IEC 42005:2025, dan ISO/IEC 42006:2025.
-  Konteks Indonesia. Membahas kewajiban UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, PP Nomor 71 Tahun 2019, SE Menkominfo Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial, serta panduan kode etik AI dari OJK.
-  Terintegrasi. Menjembatani AIMS dengan ISMS ISO/IEC 27001 dan PIMS ISO/IEC 27701 sehingga organisasi bersertifikat tidak perlu membangun sistem terpisah.
-  Aktual pada isu Generative AI. Membahas prompt injection, halusinasi, RAG, basis data vektor, AI gateway, dan AI agent yang belum banyak diulas buku tata kelola AI berbahasa Indonesia.
-  Siap pakai. 122 tabel, 23 gambar, checklist evaluasi di setiap bab, dan sepuluh lampiran template.
-  Referensi terkurasi. Lima puluh rujukan ilmiah dan regulasi, termasuk NIST AI RMF, OWASP Top 10 for LLM Applications 2025, MITRE ATLAS, ENISA, UNESCO, OECD, dan EU AI Act.