

KERANGKA KERJA PENGENDALIAN KEAMANAN INFORMASI DAN PERLINDUNGAN DATA PRIBADI PADA **IMAGE PROCESSING**

Berbasis ISO/IEC 27002 dan ISO/IEC 27701



Penulis:

Dr. Nungky Awang Chandra, S.Si., M.Ti
Dr. Hadi Santoso, S.Kom., M.Kom.
Mohamad Yusuf, S.Kom., M.C.S.
Siti Maesaroh, S.Kom., M.T.I.
Diva Aliftha Chandra, B.Eng., M.Sc.

KERANGKA KERJA PENGENDALIAN KEAMANAN INFORMASI DAN PERLINDUNGAN DATA PRIBADI PADA *IMAGE PROCESSING*

Berbasis ISO/IEC 27002 dan ISO/IEC 27701

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

Dr. Hadi Santoso, S.Kom., M.Kom.

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

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

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

KERANGKA KERJA PENGENDALIAN KEAMANAN INFORMASI DAN PERLINDUNGAN DATA PRIBADI PADA *IMAGE PROCESSING*

Berbasis ISO/IEC 27002 dan ISO/IEC 27701

Penulis:

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

Dr. Hadi Santoso, S.Kom., M.Kom.

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

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

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

Tata Letak : Lilis Khalisatul Karimah
Desain Cover : Asep Nugraha
Ukuran : UNESCO 15,5 x 23 cm
Halaman : xix, 246
ISBN : 978-634-7949-03-5
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 penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga buku berjudul Kerangka Kerja Pengendalian Keamanan Informasi dan Perlindungan Data Pribadi pada *Image processing* Berbasis ISO/IEC 27002 dan ISO/IEC 27701 ini dapat diselesaikan.

Buku ini lahir dari pengamatan atas satu kesenjangan yang berulang kali penulis jumpai dalam praktik audit, konsultasi, dan pengajaran. Organisasi mengadopsi teknologi pemrosesan citra dengan sangat cepat, mulai dari kamera pengawas, analitik video, pengenalan wajah, hingga penglihatan komputer berbasis kecerdasan buatan, sementara kematangan pengendaliannya tertinggal jauh di belakang. Kamera dipasang tanpa penilaian dampak, rekaman disimpan tanpa batas waktu, dan kemampuan analitik diaktifkan tanpa dasar pemrosesan yang jelas. Kesenjangan ini bukan disebabkan oleh ketiadaan niat baik, melainkan oleh ketiadaan panduan yang menghubungkan standar pengendalian dengan karakteristik teknis pemrosesan citra.

Buku ini berupaya mengisi kesenjangan tersebut. Pembahasan tidak berhenti pada penjelasan standar, melainkan menerjemahkan maksud kontrol menjadi rancangan penerapan yang konkret, disertai bukti implementasi dan cara pengujiannya. Setiap tabel dalam buku ini disusun agar dapat langsung disalin dan disesuaikan oleh pembaca sebagai instrumen kerja.

Penulis menyampaikan terima kasih kepada rekan-rekan di Fakultas Ilmu Komputer Universitas Mercu Buana atas diskusi akademik yang memperkaya kerangka berpikir dalam buku ini, kepada rekan-rekan di PT TSI Sertifikasi Internasional atas pengalaman lapangan yang menjadi bahan studi kasus, serta kepada Penerbit Sada Kurnia Pustaka atas kesediaannya menerbitkan karya ini.

Penulis menyadari bahwa buku ini masih memiliki kekurangan. Saran dan kritik dari pembaca sangat penulis harapkan untuk penyempurnaan pada edisi berikutnya. Semoga buku ini bermanfaat bagi praktisi, auditor, akademisi, dan seluruh pihak yang berkepentingan dengan penerapan teknologi citra yang bertanggung jawab.

Penulis

PRAKATA

Citra telah berubah kedudukannya. Jika dahulu foto dan video merupakan dokumentasi yang ditinjau ketika terjadi peristiwa, kini citra menjadi masukan bagi keputusan yang diambil secara otomatis dan berdampak langsung terhadap individu. Perubahan ini terjadi begitu cepat sehingga banyak organisasi belum sempat menyesuaikan cara mereka mengendalikannya.

Buku ini disusun berdasarkan tiga keyakinan. Keyakinan pertama, bahwa pengendalian yang efektif harus berangkat dari pemahaman teknis yang memadai. Diskusi mengenai perlindungan citra yang tidak memahami perbedaan antara templat biometrik dan berkas gambar, atau antara pseudonimisasi dan anonimisasi, akan menghasilkan kontrol yang tidak tepat sasaran. Karena itu, tiga bab pertama buku ini dicurahkan untuk membangun fondasi pemahaman tersebut.

Keyakinan kedua, bahwa keamanan informasi dan perlindungan data pribadi harus dikelola secara terpadu. Keduanya sering diperlakukan sebagai dua program terpisah dengan pemilik berbeda, padahal pada pemrosesan citra hampir setiap aset memiliki kedua dimensi sekaligus. Pemisahan menghasilkan duplikasi yang mahal sekaligus celah pada titik yang seharusnya ditangani bersama. Buku ini secara konsisten memperlakukan keduanya sebagai satu kesatuan.

Keyakinan ketiga, bahwa pengendalian yang tidak menghasilkan bukti tidak dapat diandalkan. Kontrol yang tidak menghasilkan artefak tidak dapat diuji, dan kontrol yang tidak dapat diuji tidak dapat dinyatakan berjalan. Karena itu, setiap rancangan kontrol dalam buku ini disertai penyebutan bukti implementasi dan metode pengujiannya.

Perlu ditegaskan bahwa buku ini bukan salinan maupun ringkasan dari teks standar. Teks ISO/IEC 27002 dan ISO/IEC 27701

dilindungi hak cipta dan hanya dapat diperoleh secara sah melalui badan standarisasi yang berwenang. Yang disajikan dalam buku ini adalah penafsiran penerapan, yaitu bagaimana maksud kontrol diwujudkan pada konteks spesifik pemrosesan citra. Pembaca yang menerapkan kerangka ini perlu memverifikasi nomor klausul dan penomoran kontrol terhadap edisi standar resmi yang berlaku pada organisasinya.

Akhirnya, penulis berharap buku ini dapat membantu organisasi memanfaatkan teknologi pemrosesan citra secara optimal tanpa mengorbankan hak individu yang terekam di dalamnya. Inovasi berbasis citra akan lebih bermakna apabila privasi dan keamanan menjadi bagian dari rancangannya sejak awal.

Jakarta, September 2026
Penulis

DAFTAR ISI

KATA PENGANTAR.....	iii
PRAKATA.....	v
DAFTAR ISI	vii
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xix
BAB 1 PENDAHULUAN.....	1
A. Transformasi Digital dan Pertumbuhan Penggunaan <i>Image Processing</i>	1
B. <i>Image</i> sebagai Informasi, Data, dan Bukti Digital	3
C. Tantangan Keamanan Informasi pada Foto, Video, CCTV, dan <i>Computer Vision</i>	4
D. Tantangan Perlindungan Data Pribadi dan Informasi yang Dapat Mengidentifikasi Individu.....	6
E. Urgensi Pengendalian Berbasis Risiko.....	8
F. Peran ISO/IEC 27002 dan ISO/IEC 27701	9
G. Tujuan, Ruang Lingkup, dan Sasaran Pembaca Buku	11
H. Metode dan Struktur Pembahasan Buku	12
BAB 2 KONSEP DASAR <i>IMAGE</i> DAN <i>VIDEO PROCESSING</i>	14
A. Pengertian <i>Digital Image</i> dan Video	14
B. Akuisisi dan <i>Capture Image</i>	15
C. <i>Pre-processing</i> dan <i>Enhancement</i>	17
D. <i>Segmentation</i> , <i>Feature Extraction</i> , dan <i>Classification</i>	18
E. <i>Object Detection</i> dan <i>Recognition</i>	20
F. <i>Facial Recognition</i> dan <i>Biometric Processing</i>	21
G. <i>Video Analytics</i> dan <i>CCTV Intelligence</i>	23
H. <i>Computer Vision</i> dan <i>Artificial Intelligence</i>	24
I. <i>Metadata</i> , <i>EXIF</i> , <i>Geolocation</i> , dan Informasi Tersembunyi.....	25
J. Arsitektur Sistem <i>Image processing</i> : <i>Edge</i> , <i>Server</i> , <i>Cloud</i> , dan AI.....	27
BAB 3 <i>IMAGE</i> SEBAGAI ASET INFORMASI	30
A. Konsep Aset Informasi.....	30

B.	Klasifikasi <i>Image</i> dan Video Berdasarkan Sensitivitas.....	31
C.	<i>Confidentiality, Integrity, dan Availability</i>	33
D.	<i>Authenticity, Accountability, dan Non-repudiation</i>	34
E.	Kepemilikan, <i>Custodianship</i> , dan Tanggung Jawab.....	36
F.	Inventarisasi Aset <i>Image</i> dan Video	37
G.	<i>Data Flow dan Information Flow Mapping</i>	38
H.	Nilai Bisnis, Nilai Pembuktian, dan Dampak Kebocoran	40
BAB 4 RISIKO KEAMANAN INFORMASI PADA IMAGE		
PROCESSING		42
A.	Konsep <i>Threat, Vulnerability, Likelihood, dan Impact</i>	42
B.	<i>Unauthorized Access dan Disclosure</i>	44
C.	Manipulasi, <i>Tampering</i> , dan Pemalsuan <i>Image</i>	46
D.	<i>Deepfake dan Synthetic Media</i>	47
E.	<i>Malware, Ransomware, dan Serangan terhadap Storage</i>	48
F.	<i>Interception</i> pada Kamera, <i>Network, API, dan Cloud</i>	50
G.	Risiko Model AI dan <i>Adversarial Image</i>	51
H.	Risiko <i>Third Party</i> dan <i>Supply Chain</i>	53
I.	Risiko <i>Human Error</i> dan <i>Insider Threat</i>	54
J.	Metode <i>Risk Assessment</i> untuk <i>Image Processing</i>	55
K.	Penyusunan <i>Risk Register</i>	57
BAB 5 RISIKO PRIVASI DAN PERLINDUNGAN DATA PRIBADI ...		59
A.	<i>Image</i> dan Video sebagai Data Pribadi.....	59
B.	<i>Identifiability dan Linkability</i>	60
C.	<i>Biometric Data</i> dan Data Sensitif.....	62
D.	<i>Surveillance</i> dan Risiko Pemantauan Individu	64
E.	<i>Purpose Limitation</i> dan <i>Data Minimization</i>	65
F.	<i>Transparency</i> dan Informasi kepada Subjek Data.....	67
G.	<i>Retention, Deletion, dan Secondary Use</i>	68
H.	<i>Data Sharing</i> dan <i>Cross-border Processing</i>	70
I.	<i>Privacy Risk Assessment</i> dan PIA/DPIA	71
J.	<i>Privacy by Design</i> dan <i>Privacy by Default</i>	72
BAB 6 KERANGKA KONTROL ISO/IEC 27002 UNTUK IMAGE		
PROCESSING		75
A.	Posisi ISO/IEC 27002 dalam Pengendalian Keamanan Informasi.....	75
B.	Struktur dan Atribut Kontrol	76

C.	<i>Organizational Controls</i>	78
D.	<i>People Controls</i>	80
E.	<i>Physical Controls</i>	81
F.	<i>Technological Controls</i>	83
G.	Pemilihan Kontrol Berdasarkan Risiko <i>Image Processing</i>	84
H.	<i>Control Objective, Control Design, dan Control Effectiveness</i> ..	86
I.	<i>Evidence dan Dokumentasi Implementasi</i>	87
J.	Contoh <i>Control Matrix</i> untuk <i>Image Processing</i>	88
BAB 7 KERANGKA PRIVASI ISO/IEC 27701 UNTUK IMAGE		
PROCESSING		91
A.	<i>Privacy Information Management</i> dalam Konteks <i>Image Processing</i>	91
B.	PII dan PII <i>Principal</i>	92
C.	Peran PII <i>Controller</i>	94
D.	Peran PII <i>Processor</i>	95
E.	Hubungan <i>Controller-Processor</i> dan Pihak Ketiga	97
F.	Pengelolaan Tujuan dan Dasar Pemrosesan	98
G.	Hak dan Permintaan PII <i>Principal</i>	100
H.	<i>Transfer, Disclosure, Retention, dan Disposal</i>	101
I.	<i>Privacy Governance dan Accountability</i>	103
J.	Pemetaan <i>Privacy Controls</i> untuk <i>Image</i> dan <i>Video</i>	104
BAB 8 SIKLUS HIDUP IMAGE PROCESSING DAN TITIK		
PENGENDALIAN		107
A.	<i>Image Processing Lifecycle</i>	107
B.	<i>Collection dan Capture</i>	109
C.	<i>Transmission</i>	110
D.	<i>Ingestion dan Validation</i>	111
E.	<i>Storage dan Database</i>	113
F.	<i>Processing dan Analytics</i>	115
G.	<i>AI Training dan Inference</i>	116
H.	<i>Display, Reporting, dan Visualization</i>	118
I.	<i>Sharing, Export, dan Integration</i>	119
J.	<i>Archiving, Retention, dan Destruction</i>	120
K.	<i>Control Points</i> pada Setiap Tahap <i>Lifecycle</i>	122
BAB 9 PEMETAAN KONTROL KEAMANAN INFORMASI		124
A.	Metodologi <i>Control Mapping</i>	124

B.	<i>Identity and Access Management</i>	125
C.	<i>Authentication dan Privileged Access</i>	127
D.	<i>Cryptography dan Key Management</i>	129
E.	<i>Secure Transfer dan Network Security</i>	130
F.	<i>Logging, Monitoring, dan Audit Trail</i>	132
G.	<i>Backup, Recovery, dan Availability</i>	134
H.	<i>Secure Development dan Change Management</i>	136
I.	<i>Cloud Security dan Third-party Services</i>	138
J.	<i>Physical Security Kamera dan Perangkat</i>	140
K.	<i>Incident Management dan Digital Evidence</i>	141
L.	<i>Control Matrix: Risiko - Proses - Kontrol - Evidence</i>	143
BAB 10 PEMETAAN KONTROL PRIVASI		145
A.	<i>Pemetaan PII dalam Image Processing</i>	145
B.	<i>Lawful/Purpose-based Processing dan Governance</i>	146
C.	<i>Notice dan Transparency</i>	148
D.	<i>Consent dan Preference Management bila Relevan</i>	149
E.	<i>Data Minimization</i>	151
F.	<i>Masking, Blurring, Redaction, dan Anonymization</i>	152
G.	<i>Pseudonymization dan Tokenization</i>	155
H.	<i>Retention dan Secure Deletion</i>	156
I.	<i>Data Subject/PII Principal Request</i>	158
J.	<i>Controller-Processor Control Mapping</i>	160
K.	<i>Privacy Incident dan Breach Handling</i>	162
L.	<i>Privacy Control Matrix</i>	163
BAB 11 FRAMEWORK PENGENDALIAN KEAMANAN INFORMASI DAN PRIVASI PADA IMAGE PROCESSING		166
A.	<i>Prinsip dan Tujuan Framework</i>	166
B.	<i>Governance Layer</i>	168
C.	<i>Risk and Privacy Assessment Layer</i>	169
D.	<i>Data/Image Lifecycle Layer</i>	171
E.	<i>Security and Privacy Control Layer</i>	172
F.	<i>Technology and AI Layer</i>	174
G.	<i>Human and Third-party Layer</i>	175
H.	<i>Monitoring, Measurement, dan Assurance Layer</i>	176
I.	<i>Framework Implementasi: Identify - Assess - Design - Implement - Monitor - Improve</i>	178

J. <i>Maturity Model Pengendalian Image Processing</i>	180
K. <i>KPI/KRI dan Control Effectiveness</i>	182
L. <i>Continuous Improvement</i>	184
BAB 12 STUDI KASUS, ASSESSMENT, DAN CHECKLIST	
IMPLEMENTASI	186
A. Studi Kasus CCTV di Area Publik dan Perkantoran.....	186
B. Studi Kasus <i>Facial Recognition</i>	188
C. Studi Kasus <i>Image Processing</i> untuk <i>Quality Inspection</i>	189
D. Studi Kasus <i>Healthcare/Medical Image</i>	191
E. Studi Kasus <i>Video Analytics</i> Berbasis AI	192
F. Studi Kasus <i>Cloud-based Image Processing</i>	194
G. <i>Self-assessment Checklist</i>	195
H. <i>Risk Assessment Worksheet</i>	197
I. <i>Security & Privacy Control Checklist</i>	199
J. <i>Audit Evidence Checklist</i>	201
K. <i>Gap Analysis</i> dan Prioritas Perbaikan	203
L. <i>Roadmap Implementasi 30-60-90 Hari</i>	204
LAMPIRAN A TEMPLAT ASSET REGISTER IMAGE/VIDEO	208
LAMPIRAN B TEMPLAT RISK REGISTER	210
LAMPIRAN C TEMPLAT PRIVACY IMPACT ASSESSMENT	214
LAMPIRAN D TEMPLAT CONTROL MAPPING ISO/IEC 27002	217
LAMPIRAN E TEMPLAT PRIVACY CONTROL MAPPING ISO/IEC 27701	221
LAMPIRAN F TEMPLAT AUDIT CHECKLIST DAN EVIDENCE REGISTER	225
DAFTAR PUSTAKA	229
DAFTAR SINGKATAN	232
GLOSARIUM	234
INDEKS	238
BIOGRAFI PENULIS	241

DAFTAR TABEL

Tabel 1. 1: Pergeseran Peran Citra dalam Organisasi	2
Tabel 1. 2: Tiga Kedudukan Citra dan Implikasi Pengendaliannya	4
Tabel 1. 3: Perbandingan Karakteristik Data Terstruktur dan Data Citra.....	5
Tabel 1. 4: Prinsip Perlindungan Data Pribadi dan Implikasinya pada Pemrosesan Citra.....	7
Tabel 1. 5: Perbedaan Sudut Pandang Risiko Keamanan dan Risiko Privasi	9
Tabel 1. 6: Pembagian Peran Kedua Standar dalam Buku Ini	10
Tabel 1. 7: Sasaran Pembaca dan Bagian yang Paling Relevan.....	12
Tabel 2. 1: Parameter Teknis Citra dan Video yang Memengaruhi Pengendalian	15
Tabel 2. 2: Keputusan Akuisisi dan Dampaknya terhadap Risiko	16
Tabel 2. 3: Operasi Prapemrosesan dan Pertimbangan Pengendaliannya.....	18
Tabel 2. 4: Keluaran Setiap Tahap Analisis dan Klasifikasi Sensitivitasnya.....	19
Tabel 2. 5: Tingkatan Analisis Objek dan Kebutuhan Data Pribadi	20
Tabel 2. 6: Perbandingan Mode Verifikasi dan Identifikasi Biometrik	22
Tabel 2. 7: Perubahan Risiko akibat Penerapan Analitik Video	23
Tabel 2. 8: Komponen Sistem Kecerdasan Buatan Berbasis Citra sebagai Aset.....	24
Tabel 2. 9: Kategori Metadata pada Berkas Citra dan Potensi Risikonya	26
Tabel 2. 10: Perbandingan Profil Risiko Tiga Pola Arsitektur.....	28
Tabel 3. 1: Kategori Aset dalam Ekosistem Pemrosesan Citra.....	31
Tabel 3. 2: Skema Klasifikasi Citra dan Video	32
Tabel 3. 3: Perwujudan Sifat Keamanan pada Aset Citra.....	33
Tabel 3. 4: Mekanisme Pendukung Keaslian dan Nirsangkal	35
Tabel 3. 5: Pembagian Peran dan Tanggung Jawab atas Aset Citra....	36
Tabel 3. 6: Atribut Minimum Inventaris Aset Citra	38

Tabel 3. 7: Titik Rawan yang Sering Ditemukan melalui Pemetaan Aliran	39
Tabel 3. 8: Matriks Penilaian Aset Citra pada Tiga Dimensi.....	40
Tabel 4. 1: Skala Kemungkinan yang Digunakan dalam Buku Ini.....	43
Tabel 4. 2: Skala Dampak yang Digunakan dalam Buku Ini.....	43
Tabel 4. 3: Skenario Risiko Akses Tidak Sah dan Penilaiannya.....	45
Tabel 4. 4: Kontrol Deteksi Manipulasi dan Keterbatasannya.....	46
Tabel 4. 5: Skenario Risiko Media Sintetis	47
Tabel 4. 6: Skenario Risiko Perangkat Lunak Berbahaya pada Ekosistem Citra.....	49
Tabel 4. 7: Skenario Risiko Penyesuaian dan Penilaiannya	50
Tabel 4. 8: Skenario Risiko pada Model Kecerdasan Buatan	52
Tabel 4. 9: Pihak Ketiga dalam Ekosistem Pemrosesan Citra dan Risikonya	53
Tabel 4. 10: Skenario Risiko Faktor Manusia	55
Tabel 4. 11: Matriks Risiko Lima Kali Lima yang Digunakan.....	56
Tabel 4. 12: Kriteria Tingkat dan Penerimaan Risiko	57
Tabel 4. 13: Struktur Kolom Daftar Risiko yang Disarankan.....	57
Tabel 5. 1: Kondisi yang Menjadikan Citra sebagai Data Pribadi	60
Tabel 5. 2: Tingkatan Keteridentifikasi dan Konsekuensinya.....	61
Tabel 5. 3: Jenis Data Biometrik pada Pemrosesan Citra dan Tingkat Risikonya	62
Tabel 5. 4: Kriteria Kewajaran Pengawasan pada Lingkungan Kerja	64
Tabel 5. 5: Perbandingan Rumusan Tujuan yang Tidak Memadai dan Memadai.....	66
Tabel 5. 6: Dimensi Minimalisasi pada Pemrosesan Citra.....	66
Tabel 5. 7: Isi Minimum Pemberitahuan pada Setiap Lapis	67
Tabel 5. 8: Acuan Penetapan Masa Simpan Berdasarkan Tujuan.....	68
Tabel 5. 9: Bentuk Pembagian Data Citra dan Persyaratannya.....	70
Tabel 5. 10: Tahapan Pelaksanaan Penilaian Dampak Perlindungan Data	71
Tabel 5. 11: Penerapan Privasi sejak Perancangan pada Setiap Keputusan Arsitektur	73
Tabel 6. 1: Kedudukan Standar dalam Kerangka Pengendalian.....	76
Tabel 6. 2: Empat Tema Kontrol dan Relevansinya pada Pemrosesan Citra.....	77

Tabel 6. 3: Atribut Kontrol dan Nilai yang Dimungkinkan.....	77
Tabel 6. 4: Kontrol Organisasional Utama pada Pemrosesan Citra.....	78
Tabel 6. 5: Kontrol Orang dan Penerapannya pada Pemrosesan Citra.....	80
Tabel 6. 6: Kontrol Fisik dan Penerapannya pada Pemrosesan Citra.....	81
Tabel 6. 7: Kontrol Teknologi dan Penerapannya pada Pemrosesan Citra.....	83
Tabel 6. 8: Contoh Pemetaan Risiko ke Kontrol Terpilih.....	85
Tabel 6. 9: Contoh Penguraian Tiga Tingkatan pada Satu Kontrol	86
Tabel 6. 10: Jenis Bukti dan Karakteristiknya.....	87
Tabel 6. 11: Matriks Kontrol Keamanan Informasi untuk Pemrosesan Citra.....	89
Tabel 7. 1: Perluasan yang Diberikan Kerangka Privasi terhadap Kerangka Keamanan	92
Tabel 7. 2: Kategori Subjek Data pada Pemrosesan Citra.....	93
Tabel 7. 3: Kewajiban Utama Pengendali pada Pemrosesan Citra.....	94
Tabel 7. 4: Kewajiban Utama Pemroses pada Pemrosesan Citra.....	96
Tabel 7. 5: Penentuan Peran pada Situasi yang Lazim Ditemukan.....	97
Tabel 7. 6: Pemetaan Tujuan dan Dasar Pemrosesan pada Pengawasan Visual	99
Tabel 7. 7: Hak Subjek Data dan Tantangan Pemenuhannya pada Citra.....	100
Tabel 7. 8: Register Pengungkapan Informasi Pribadi.....	102
Tabel 7. 9: Unsur Tata Kelola Privasi dan Bukti Pendukungnya.....	103
Tabel 7. 10: Matriks Kontrol Privasi untuk Pemrosesan Citra.....	104
Tabel 8. 1: Sembilan Tahap Siklus Hidup dan Ciri Risikonya	108
Tabel 8. 2: Kontrol pada Tahap Pengumpulan beserta Buktinya	110
Tabel 8. 3: Segmen Transmisi dan Kontrol yang Berlaku.....	110
Tabel 8. 4: Kontrol pada Tahap Penerimaan dan Validasi	112
Tabel 8. 5: Lapis Penyimpanan dan Kontrol yang Berlaku	114
Tabel 8. 6: Tingkat Kerincian Keluaran Analitik dan Pemilihannya.....	115
Tabel 8. 7: Kontrol pada Tahap Pelatihan dan Inferensi.....	117
Tabel 8. 8: Risiko dan Kontrol pada Tahap Penyajian.....	118
Tabel 8. 9: Bentuk Integrasi dan Pertimbangan Pengendaliannya.....	120
Tabel 8. 10: Perbedaan Pengarsipan dan Retensi Operasional	121
Tabel 8. 11: Peta Titik Kendali Sepanjang Siklus Hidup.....	122

Tabel 9. 1: Struktur Baku Setiap Entri Pemetaan Kontrol.....	124
Tabel 9. 2: Matriks Peran dan Hak Akses pada Sistem Manajemen Video	126
Tabel 9. 3: Pemetaan Kontrol Pengelolaan Identitas dan Akses	126
Tabel 9. 4: Pemetaan Kontrol Autentikasi dan Akses Istimewa.....	128
Tabel 9. 5: Penerapan Kriptografi pada Setiap Tahap Siklus Hidup	129
Tabel 9. 6: Pemetaan Kontrol Kriptografi dan Pengelolaan Kunci...	130
Tabel 9. 7: Pemetaan Kontrol Keamanan Jaringan	131
Tabel 9. 8: Peristiwa yang Wajib Tercatat pada Sistem Pemrosesan Citra.....	132
Tabel 9. 9: Pemetaan Kontrol Pencatatan dan Pemantauan	133
Tabel 9. 10: Pemetaan Kontrol Ketersediaan dan Pemulihan.....	135
Tabel 9. 11: Pemetaan Kontrol Pengembangan dan Manajemen Perubahan.....	137
Tabel 9. 12: Pembagian Tanggung Jawab pada Penggunaan Layanan Awan.....	138
Tabel 9. 13: Pemetaan Kontrol Layanan Awan dan Pihak Ketiga.....	139
Tabel 9. 14: Pemetaan Kontrol Keamanan Fisik.....	140
Tabel 9. 15: Pemetaan Kontrol Manajemen Insiden dan Bukti Digital	142
Tabel 9. 16: Matriks Terpadu Risiko, Proses, Kontrol, dan Bukti	143
Tabel 10. 1: Bentuk Informasi Pribadi pada Ekosistem Pemrosesan Citra.....	145
Tabel 10. 2: Pemetaan Kontrol Dasar dan Tujuan Pemrosesan	147
Tabel 10. 3: Pemetaan Kontrol Transparansi.....	148
Tabel 10. 4: Syarat Persetujuan yang Sah dan Kendalanya pada Citra.....	149
Tabel 10. 5: Pemetaan Kontrol Persetujuan dan Preferensi.....	150
Tabel 10. 6: Pemetaan Kontrol Minimalisasi pada Setiap Dimensi .	151
Tabel 10. 7: Perbandingan Teknik Penyamaran Visual.....	153
Tabel 10. 8: Pemetaan Kontrol Penyamaran Visual.....	154
Tabel 10. 9: Penerapan Pseudonimisasi pada Komponen Sistem....	155
Tabel 10. 10: Pemetaan Kontrol Pseudonimisasi dan Tokenisasi....	156
Tabel 10. 11: Pemetaan Kontrol Retensi dan Penghapusan	157
Tabel 10. 12: Alur Penanganan Permintaan Subjek Data.....	158

Tabel 10. 13: Pemetaan Kontrol Penanganan Permintaan Subjek Data	159
Tabel 10. 14: Pembagian Kontrol antara Pengendali dan Pemroses	160
Tabel 10. 15: Pemetaan Kontrol Pengelolaan Pemroses	161
Tabel 10. 16: Pemetaan Kontrol Penanganan Insiden Privasi	162
Tabel 10. 17: Matriks Terpadu Kontrol Privasi	164
Tabel 11. 1: Komponen Lapisan Tata Kelola.....	168
Tabel 11. 2: Proses Terpadu Penilaian Risiko dan Dampak.....	170
Tabel 11. 3: Fungsi Lapisan Siklus Hidup dalam Kerangka Kerja	171
Tabel 11. 4: Struktur Himpunan Kontrol Terpadu	172
Tabel 11. 5: Contoh Pertahanan Berlapis terhadap Kebocoran Rekaman.....	173
Tabel 11. 6: Komponen Pengendalian pada Lapisan Teknologi dan AI	174
Tabel 11. 7: Komponen Lapisan Manusia dan Pihak Ketiga.....	175
Tabel 11. 8: Tiga Lini Pemastian pada Kerangka Kerja	177
Tabel 11. 9: Enam Tahap Siklus Penerapan	178
Tabel 11. 10: Lima Tingkat Kematangan dan Cirinya.....	180
Tabel 11. 11: Indikator Kematangan pada Setiap Lapisan.....	181
Tabel 11. 12: Indikator Kinerja Pengendalian yang Disarankan	182
Tabel 11. 13: Indikator Risiko yang Perlu Dipantau.....	183
Tabel 11. 14: Sumber Masukan bagi Perbaikan Berkelanjutan.....	184
Tabel 12. 1: Penilaian Risiko Ringkas Studi Kasus Perkantoran.....	187
Tabel 12. 2: Perbandingan Rancangan Awal dan Rancangan Perbaikan	188
Tabel 12. 3: Prioritas Kontrol pada Kasus Inspeksi Mutu.....	190
Tabel 12. 4: Perbandingan Pengendalian Dua Sistem pada Rumah Sakit	191
Tabel 12. 5: Penyesuaian Rancangan Layanan Analitik	193
Tabel 12. 6: Penilaian Aspek Kunci Penggunaan Layanan Awan.....	194
Tabel 12. 7: Daftar Periksa Penilaian Mandiri Lapisan Tata Kelola dan Aset.....	195
Tabel 12. 8: Daftar Periksa Penilaian Mandiri Lapisan Risiko dan Kontrol Keamanan.....	196
Tabel 12. 9: Daftar Periksa Penilaian Mandiri Lapisan Privasi.....	196

Tabel 12. 10: Penafsiran Skor Penilaian Mandiri	197
Tabel 12. 11: Bagian Pertama Lembar Kerja Konteks Aliran	198
Tabel 12. 12: Bagian Kedua Lembar Kerja Penilaian Skenario.....	198
Tabel 12. 13: Daftar Periksa Kontrol Tahap Pengumpulan dan Transmisi	199
Tabel 12. 14: Daftar Periksa Kontrol Tahap Penyimpanan dan Pengolahan.....	200
Tabel 12. 15: Daftar Periksa Kontrol Tahap Pembagian dan Pemusnahan	200
Tabel 12. 16: Bukti Tingkat Tata Kelola.....	201
Tabel 12. 17: Bukti Tingkat Risiko dan Kontrol	201
Tabel 12. 18: Bukti Tingkat Privasi	202
Tabel 12. 19: Matriks Prioritas Penanganan Kesenjangan	203
Tabel 12. 20: Contoh Hasil Analisis Kesenjangan dan Prioritasnya	203
Tabel 12. 21: Kegiatan Tiga Puluh Hari Pertama.....	205
Tabel 12. 22: Kegiatan Hari Ketiga Puluh Satu sampai Keenam Puluh	206
Tabel 12. 23: Kegiatan Hari Keenam Puluh Satu sampai Kesembilan Puluh	206
Tabel L.A. 1: Struktur Kolom <i>Asset Register Image</i> dan <i>Video</i>	208
Tabel L.B. 1: Struktur Kolom <i>Risk Register</i> Terpadu.....	210
Tabel L.B. 2: Contoh Entri <i>Risk Register</i> Kategori Keamanan Informasi	211
Tabel L.B. 3: Contoh Entri Risk Register Kategori Privasi.....	212
Tabel L.C. 1: Bagian Satu Identifikasi Kegiatan Pemrosesan	214
Tabel L.C. 2: Bagian Dua Uji Kebutuhan dan Proporsionalitas	214
Tabel L.C. 3: Bagian Tiga Identifikasi dan Penilaian Risiko terhadap Individu.....	215
Tabel L.C. 4: Bagian Empat Kesimpulan dan Persetujuan.....	215
Tabel L.D. 1: Struktur Kolom <i>Control Mapping</i>	217
Tabel L.D. 2: Matriks Control Mapping Domain Tata Kelola dan Aset.....	218
Tabel L.D. 3: Matriks Control Mapping Domain Teknologi.....	218
Tabel L.E. 1: Matriks <i>Privacy Control Mapping Domain</i> Tujuan dan Transparansi.....	221

Tabel L.E. 2: Matriks *Privacy Control Mapping Domain* Minimalisasi dan Retensi.....222

Tabel L.E. 3: Matriks *Privacy Control Mapping Domain* Hak Subjek dan Pemroses.....223

Tabel L.F. 1: Struktur Kolom Audit *Checklist*225

Tabel L.F. 2: Butir Audit Domain Tata Kelola dan Aset.....225

Tabel L.F. 3: Butir Audit Domain Kontrol Teknis.....226

Tabel L.F. 4: Butir Audit Domain Privasi.....227

Tabel L.F. 5: Struktur Evidence Register228

DAFTAR GAMBAR

Gambar 1. 1: Struktur Pembahasan Buku.....	13
Gambar 2. 1 Pola Arsitektur Sistem Pemrosesan Citra	28
Gambar 3. 1: Rantai Keaslian Citra dari Akuisisi sampai Penyajian...	35
Gambar 4. 1: Hubungan Ancaman, Kerentanan, Aset, dan Dampak...	43
Gambar 5. 1: Spektrum Keteridentifikasian pada Citra.....	61
Gambar 6. 1: Empat Tema Kontrol dan Distribusinya	77
Gambar 7. 1: Hubungan Subjek Data, Pengendali, dan Pemroses.....	97
Gambar 8. 1: Sembilan Tahap Siklus Hidup Pemrosesan Citra.....	108
Gambar 10. 1: Spektrum Teknik De-identifikasi Visual	153
Gambar 11. 1: Kerangka Kerja Pengendalian Tujuh Lapisan	168
Gambar 11. 2: Lima Tingkat Kematangan Pengendalian.....	180
Gambar 12. 1: Peta Jalan Implementasi Tiga Puluh, Enam Puluh, dan Sembilan Puluh Hari.....	205

BAB 1

PENDAHULUAN

A. Transformasi Digital dan Pertumbuhan Penggunaan *Image Processing*

Transformasi digital yang berlangsung dalam dua dekade terakhir telah mengubah cara organisasi mengumpulkan, mengolah, dan memanfaatkan informasi. Jika sebelumnya informasi organisasi didominasi oleh data terstruktur berupa angka dan teks dalam basis data transaksional, saat ini porsi terbesar dari data yang dihasilkan justru berbentuk tidak terstruktur, dan sebagian besar di antaranya adalah citra dan video. Kamera pengawas, kamera ponsel, kamera pada kendaraan, perangkat medis pencitraan, sensor visual pada lini produksi, hingga kamera pada perangkat *wearable* menghasilkan aliran citra yang terus-menerus dan dalam volume yang sangat besar.

Pertumbuhan ini tidak hanya bersifat kuantitatif. Perubahan yang lebih mendasar terjadi pada sisi pemanfaatan. Citra tidak lagi sekadar disimpan sebagai arsip pasif yang ditinjau ketika terjadi insiden, melainkan diproses secara otomatis dan *real time* untuk menghasilkan keputusan. Sistem video *analytics* mengenali pola pergerakan, sistem pengenalan wajah mencocokkan identitas, sistem inspeksi visual menentukan lolos atau tidaknya suatu produk, dan sistem pencitraan medis membantu menegakkan diagnosis. Citra telah berubah dari objek dokumentasi menjadi masukan bagi proses pengambilan keputusan yang berdampak langsung terhadap individu maupun organisasi.

Perubahan peran ini didorong oleh tiga faktor yang saling menguatkan. Faktor pertama adalah penurunan biaya perangkat akuisisi. Kamera dengan resolusi tinggi kini tersedia dengan harga yang jauh lebih

terjangkau dibandingkan satu dekade lalu, sehingga organisasi dapat memasang perangkat dalam jumlah besar tanpa beban investasi yang berlebihan. Faktor kedua adalah ketersediaan kapasitas komputasi, khususnya akselerator berbasis GPU dan perangkat *edge* yang mampu menjalankan model pembelajaran mesin di lokasi akuisisi. Faktor ketiga adalah kematangan algoritma *computer vision* berbasis *deep learning* yang meningkatkan akurasi pengenalan objek dan wajah hingga tingkat yang layak untuk penggunaan operasional.

Tabel 1. 1: Pergeseran Peran Citra dalam Organisasi

Aspek	Paradigma Lama	Paradigma Saat Ini
Fungsi citra	Dokumentasi dan arsip	Masukan keputusan otomatis
Volume	Terbatas, per kejadian	Kontinu, <i>streaming</i>
Pemrosesan	Manual oleh manusia	Otomatis oleh algoritma
Lokasi olah	Terpusat	<i>Edge</i> , server, dan <i>cloud</i>
Retensi	Singkat, ditimpa berkala	Panjang untuk pelatihan model
Dampak kesalahan	Terbatas pada dokumen	Keputusan yang mengenai individu

Sumber: Diolah Penulis

Konsekuensi dari pergeseran tersebut bersifat dua arah. Di satu sisi, organisasi memperoleh manfaat efisiensi, kecepatan, dan konsistensi yang sulit dicapai melalui pengamatan manusia. Di sisi lain, organisasi kini menyimpan dan mengolah informasi yang secara inheren mengandung identitas individu, perilaku, lokasi, dan bahkan kondisi kesehatan, dalam volume yang jauh melampaui kemampuan pengawasan konvensional. Ketidakseimbangan antara kecepatan adopsi teknologi dan kematangan pengendaliannya inilah yang menjadi titik berangkat pembahasan dalam buku ini.

Fenomena serupa tampak pada tingkat nasional. Penerapan sistem pengawasan berbasis kamera pada ruang publik, penggunaan verifikasi wajah pada layanan keuangan digital, serta pemanfaatan analitik video pada sektor transportasi dan ritel berkembang lebih cepat daripada penyusunan kebijakan internal yang mengaturnya. Banyak organisasi telah mengoperasikan sistem pemrosesan citra selama bertahun-tahun

tanpa pernah melakukan inventarisasi aset citra, penilaian risiko privasi, maupun penetapan periode retensi yang eksplisit.

B. *Image sebagai Informasi, Data, dan Bukti Digital*

Untuk dapat mengendalikan citra secara tepat, terlebih dahulu perlu dipahami bahwa satu berkas citra dapat menempati tiga posisi yang berbeda secara bersamaan. Ketiga posisi tersebut menuntut perlakuan pengendalian yang berbeda pula, dan kegagalan membedakannya merupakan salah satu penyebab paling umum dari kontrol yang tidak tepat sasaran.

1. Citra sebagai informasi

Sebagai informasi, citra memiliki makna dan nilai bagi organisasi. Rekaman kamera pada area produksi memberi informasi mengenai kepatuhan prosedur kerja, rekaman kamera pada gerbang masuk memberi informasi mengenai kehadiran, dan citra hasil inspeksi memberi informasi mengenai mutu produk. Dalam kedudukan ini, citra tunduk pada prinsip keamanan informasi yang berlaku umum, yaitu kerahasiaan, keutuhan, dan ketersediaan.

2. Citra sebagai data pribadi

Ketika citra memuat wajah, plat nomor kendaraan, tanda tangan, dokumen identitas, atau ciri fisik lain yang memungkinkan seseorang dikenali, citra tersebut berkedudukan sebagai data pribadi. Pada citra yang memuat ciri biometrik seperti wajah, iris, atau sidik jari, kedudukannya meningkat menjadi data pribadi yang bersifat spesifik dan menuntut perlindungan yang lebih ketat. Dalam kedudukan ini, citra tunduk pada prinsip perlindungan data pribadi, antara lain pembatasan tujuan, minimalisasi data, transparansi, dan pembatasan masa simpan.

3. Citra sebagai bukti digital

Citra kerap digunakan untuk membuktikan suatu peristiwa, baik dalam proses internal seperti investigasi disiplin, maupun dalam proses eksternal seperti klaim asuransi dan proses hukum. Dalam kedudukan ini, nilai citra bergantung sepenuhnya pada kemampuan organisasi membuktikan keaslian dan keutuhannya. Rekaman yang tidak dapat dipastikan belum diubah sejak diambil kehilangan nilai pembuktiannya, betapapun jelas gambarnya.

Tabel 1. 2: Tiga Kedudukan Citra dan Implikasi Pengendaliannya

Kedudukan	Prinsip Dominan	Kontrol Kunci	Kegagalan Tipikal
Informasi	Kerahasiaan, keutuhan, ketersediaan	Klasifikasi, kontrol akses, cadangan	Berbagi tanpa kendali
Data pribadi	Pembatasan tujuan dan masa simpan	Minimalisasi, pengaburan, penghapusan	Retensi tanpa batas waktu
Bukti digital	Keaslian dan nirsangkal	Hash, watermark, rantai penyimpanan	Metadata waktu tidak tepercaya

Sumber: Diolah Penulis

Ketiga kedudukan tersebut tidak saling menggantikan. Satu rekaman kamera pada area publik dapat berkedudukan sekaligus sebagai informasi operasional, data pribadi bagi setiap orang yang terekam, dan calon bukti digital apabila terjadi insiden. Kerangka pengendalian yang memadai karenanya harus mampu mengakomodasi ketiganya secara simultan, bukan memilih salah satu dan mengabaikan yang lain.

Dimensi tambahan yang sering luput adalah metadata. Berkas citra digital umumnya membawa metadata teknis seperti model perangkat, pengaturan lensa, cap waktu, dan pada banyak kasus koordinat geografis. Metadata ini merupakan informasi tersendiri yang dapat mengungkap pola pergerakan individu meskipun isi gambarnya tidak memuat wajah. Pengendalian yang hanya berfokus pada isi visual dan mengabaikan metadata memberikan perlindungan yang tidak lengkap.

C. Tantangan Keamanan Informasi pada Foto, Video, CCTV, dan *Computer Vision*

Pengamanan citra menghadapi sejumlah karakteristik teknis yang tidak dijumpai pada data terstruktur. Karakteristik inilah yang menyebabkan penerapan kontrol keamanan standar secara apa adanya sering kali tidak efektif ketika diterapkan pada lingkungan pemrosesan citra.

1. Volume dan laju data

Satu kamera dengan resolusi tinggi dapat menghasilkan berkas berukuran belasan gigabita per hari. Organisasi dengan ratusan

kamera menghadapi laju data yang menyulitkan penerapan kontrol yang membutuhkan pemeriksaan menyeluruh, seperti pemindaian isi, klasifikasi otomatis, atau enkripsi tingkat berkas dengan kunci per objek. Keterbatasan ini mendorong sebagian organisasi menurunkan tingkat pengendalian demi menjaga kinerja sistem.

2. Distribusi titik akuisisi

Berbeda dengan basis data yang terpusat, kamera tersebar secara fisik, sering kali pada lokasi yang tidak diawasi, dan terhubung melalui jaringan yang tidak selalu tersegmentasi. Perangkat kamera kerap dikirim dengan kredensial bawaan, antarmuka manajemen yang terbuka, serta perangkat tegar yang jarang diperbarui. Titik akuisisi dengan demikian menjadi permukaan serangan yang luas sekaligus paling lemah pengawasannya.

3. Ketergantungan pada pihak ketiga

Rantai pemrosesan citra jarang berada sepenuhnya dalam kendali satu organisasi. Pemasangan dan pemeliharaan kamera umumnya dialihkan kepada penyedia jasa, penyimpanan sering ditempatkan pada layanan awan, dan kemampuan analitik kerap diperoleh melalui antarmuka pemrograman milik penyedia model. Setiap penyerahan ini memperpanjang rantai kepercayaan dan memperbesar kemungkinan kebocoran di luar batas kendali langsung organisasi.

4. Sifat data yang mudah disebar

Sekali sebuah citra keluar dari lingkungan terkendali, penyebarannya hampir tidak dapat dihentikan. Citra dapat disalin tanpa kehilangan mutu, dikirim melalui kanal apa pun, dan dipahami tanpa memerlukan konteks tambahan. Berbeda dengan tabel basis data yang memerlukan penafsiran, sebuah foto langsung bermakna bagi siapa pun yang melihatnya. Dampak kebocoran karenanya bersifat langsung dan sukar dipulihkan.

Tabel 1. 3: Perbandingan Karakteristik Data Terstruktur dan Data Citra

Karakteristik	Data Terstruktur	Data Citra dan Video
Volume per unit	Kilobita	Megabita hingga gigabita
Titik akuisisi	Aplikasi terpusat	Perangkat tersebar
Klasifikasi isi	Berdasarkan skema kolom	Memerlukan analisis isi

Karakteristik	Data Terstruktur	Data Citra dan Video
Enkripsi	Tingkat kolom dan basis data	Beban komputasi tinggi
Penghapusan selektif	Perintah pada baris	Sulit pada rekaman berkelanjutan
Kemudahan pemahaman	Perlu konteks	Langsung bermakna

Sumber: Diolah Penulis

Konsekuensi praktisnya adalah bahwa kontrol keamanan yang efektif pada lingkungan pemrosesan citra harus dirancang dengan mempertimbangkan keterbatasan tersebut sejak awal, bukan diadopsi dari lingkungan basis data lalu dipaksakan penerapannya. Buku ini secara konsisten menempatkan pertimbangan tersebut dalam setiap pembahasan pemetaan kontrol.

D. Tantangan Perlindungan Data Pribadi dan Informasi yang Dapat Mengidentifikasi Individu

Tantangan pada ranah perlindungan data pribadi berbeda sifatnya. Persoalan utamanya bukan pada kemampuan teknis melindungi berkas, melainkan pada penentuan batas kewajaran pemrosesan itu sendiri. Sebuah sistem dapat diamankan dengan sangat baik namun tetap melanggar prinsip perlindungan data pribadi apabila memproses citra melampaui tujuan yang sah.

Persoalan pertama adalah pengumpulan yang tidak terhindarkan. Kamera pada ruang publik merekam siapa pun yang melintas tanpa kemungkinan menyaring terlebih dahulu. Organisasi tidak dapat memilih untuk hanya merekam individu yang relevan. Akibatnya, pemrosesan citra hampir selalu melibatkan data individu yang tidak memiliki hubungan apa pun dengan organisasi dan tidak menyadari bahwa dirinya terekam.

Persoalan kedua adalah keterbatasan mekanisme persetujuan. Pada sebagian besar penerapan kamera pengawas, memperoleh persetujuan dari setiap subjek data secara praktis tidak mungkin. Organisasi karenanya perlu bersandar pada dasar pemrosesan lain, seperti kepentingan yang sah atau kewajiban hukum, dan hal ini

menuntut analisis penyeimbangan yang terdokumentasi, bukan sekadar asumsi bahwa pemasangan kamera lazim dilakukan.

Persoalan ketiga adalah sifat permanen data biometrik. Kata sandi yang bocor dapat diganti, nomor rekening dapat ditutup, tetapi ciri wajah seseorang tidak dapat diubah. Kebocoran templat biometrik menimbulkan kerugian yang berlaku seumur hidup subjek data. Karena itu, pemrosesan biometrik menuntut tingkat kehati-hatian yang secara kategoris lebih tinggi daripada pemrosesan data pribadi biasa.

Persoalan keempat adalah kemungkinan penggunaan sekunder. Rekaman yang semula dikumpulkan untuk tujuan keamanan fisik dengan mudah dimanfaatkan untuk mengevaluasi produktivitas pegawai, mengukur durasi istirahat, atau melatih model kecerdasan buatan. Perpindahan tujuan semacam ini kerap terjadi tanpa kajian formal dan merupakan salah satu bentuk pelanggaran prinsip pembatasan tujuan yang paling sering ditemukan dalam praktik.

Tabel 1. 4: Prinsip Perlindungan Data Pribadi dan Implikasinya pada Pemrosesan Citra

Prinsip	Implikasi pada Citra dan Video
Pembatasan tujuan	Rekaman keamanan tidak dipakai menilai kinerja
Minimalisasi data	Sudut dan resolusi kamera dibatasi seperlunya
Akurasi	Hasil pengenalan wajah diverifikasi sebelum ditindaklanjuti
Pembatasan penyimpanan	Periode retensi ditetapkan dan dijalankan otomatis
Integritas dan kerahasiaan	Enkripsi saat transit dan saat diam
Akuntabilitas	Terdapat bukti kajian dampak dan keputusan pemrosesan

Sumber: Diolah Penulis

Persoalan kelima adalah pelaksanaan hak subjek data. Ketika seseorang meminta akses terhadap rekaman yang memuat dirinya, organisasi menghadapi dilema teknis dan hukum sekaligus, karena rekaman tersebut umumnya juga memuat individu lain. Pemenuhan hak satu pihak dapat melanggar hak pihak lain apabila tidak disertai

kemampuan pengaburan selektif. Kesiapan menjawab permintaan semacam ini merupakan indikator kematangan yang jarang diuji sebelum permintaan pertama benar-benar diterima.

E. Urgensi Pengendalian Berbasis Risiko

Menghadapi keragaman tantangan tersebut, organisasi menghadapi keterbatasan sumber daya yang nyata. Tidak seluruh kamera, tidak seluruh aliran citra, dan tidak seluruh proses analitik dapat diberi tingkat perlindungan tertinggi. Pilihan yang tersedia adalah menetapkan prioritas, dan penetapan prioritas yang dapat dipertanggungjawabkan hanya dapat dilakukan melalui pendekatan berbasis risiko.

Pendekatan berbasis risiko berangkat dari pertanyaan mengenai apa yang dilindungi, dari ancaman apa, dengan kemungkinan seberapa besar, dan dengan dampak seperti apa. Jawaban atas pertanyaan tersebut menentukan kontrol mana yang diterapkan lebih dahulu dan pada tingkat apa. Pendekatan ini berbeda dari pendekatan berbasis kepatuhan yang menerapkan seluruh butir daftar periksa secara seragam tanpa memperhatikan konteks penggunaannya.

Pada lingkungan pemrosesan citra, pendekatan berbasis risiko memiliki keunggulan tambahan. Sebaran risiko pada lingkungan ini sangat tidak merata. Kamera yang mengarah ke area parkir kendaraan bermuatan risiko yang jauh berbeda dari kamera yang mengarah ke ruang perawatan pasien atau ke area penyimpanan dokumen rahasia. Perlakuan yang seragam terhadap keduanya menghasilkan pemborosan pada satu sisi dan kekurangan perlindungan pada sisi lain.

Dalam buku ini, penilaian risiko dilakukan pada dua sumbu yang berjalan bersama. Sumbu pertama adalah risiko keamanan informasi, yaitu risiko terhadap organisasi berupa kerugian operasional, finansial, maupun reputasi. Sumbu kedua adalah risiko privasi, yaitu risiko terhadap individu berupa hilangnya kendali atas informasi mengenai dirinya, pengawasan berlebihan, diskriminasi, atau kerugian akibat penyalahgunaan identitas. Kedua sumbu ini tidak selalu bergerak searah.

Tabel 1. 5: Perbedaan Sudut Pandang Risiko Keamanan dan Risiko Privasi

Aspek	Risiko Keamanan Informasi	Risiko Privasi
Pihak yang dirugikan	Organisasi	Individu subjek data
Pemicu utama	Ancaman terhadap aset	Pemrosesan yang berlebihan
Contoh kejadian	Server rekaman diretas	Rekaman dipakai di luar tujuan
Ukuran dampak	Kerugian dan gangguan layanan	Hilangnya kendali dan otonomi
Kontrol dominan	Kontrol ISO/IEC 27002	Kontrol ISO/IEC 27701

Sumber: Diolah Penulis

Sebuah sistem yang sangat aman dapat tetap menimbulkan risiko privasi yang tinggi apabila mengumpulkan lebih banyak citra daripada yang diperlukan. Sebaliknya, sistem yang meminimalkan pengumpulan tetap berisiko tinggi bagi organisasi apabila rekaman yang sedikit itu tidak terlindungi. Karena itu, kedua sumbu harus dinilai secara terpisah lalu disatukan dalam satu daftar prioritas penanganan. Pendekatan inilah yang menjadi tulang punggung kerangka kerja yang disusun pada Bab 11.

F. Peran ISO/IEC 27002 dan ISO/IEC 27701

Buku ini menggunakan dua standar internasional sebagai rujukan kontrol. Pemilihan ini didasarkan pada pertimbangan bahwa keduanya bersifat saling melengkapi dan telah diterima secara luas sebagai acuan praktik terbaik pada ranah masing-masing.

ISO/IEC 27002 menyediakan katalog kontrol keamanan informasi beserta panduan penerapannya. Edisi terkini menyusun kontrol ke dalam empat tema, yaitu kontrol organisasional, kontrol orang, kontrol fisik, dan kontrol teknologi. Setiap kontrol dilengkapi atribut yang memudahkan penyaringan menurut tipe kontrol, sifat keamanan informasi yang dilindungi, konsep keamanan siber, kapabilitas operasional, dan domain keamanan. Struktur atribut inilah yang dimanfaatkan dalam buku ini untuk menyaring kontrol yang relevan dengan pemrosesan citra.

ISO/IEC 27701 menyediakan persyaratan dan panduan untuk sistem manajemen informasi privasi. Standar ini memperluas kerangka manajemen keamanan informasi dengan menambahkan kontrol khusus bagi pengendali informasi pribadi dan bagi pemroses informasi pribadi. Pemisahan peran tersebut sangat penting dalam konteks pemrosesan citra karena satu organisasi dapat berperan sebagai pengendali atas rekaman kameranya sendiri sekaligus sebagai pemroses atas rekaman milik klien yang dianalisisnya.

Tabel 1. 6: Pembagian Peran Kedua Standar dalam Buku Ini

Aspek Pembahasan	ISO/IEC 27002	ISO/IEC 27701
Objek perlindungan	Aset informasi citra	Informasi pribadi dalam citra
Fokus kontrol	Akses, kriptografi, jejak audit	Tujuan, minimalisasi, hak subjek
Peran yang diatur	Pemilik dan kustodian aset	Pengendali dan pemroses
Keluaran utama	Pernyataan keberlakuan kontrol	Kebijakan dan catatan pemrosesan
Bab pembahasan	Bab 6 dan Bab 9	Bab 7 dan Bab 10

Sumber: Diolah Penulis

Perlu ditegaskan bahwa buku ini bukan salinan atau ringkasan dari kedua standar tersebut. Teks standar dilindungi hak cipta dan hanya dapat diperoleh secara sah melalui badan standardisasi yang berwenang. Yang disajikan dalam buku ini adalah penafsiran penerapan, yaitu bagaimana maksud dari kontrol-kontrol tersebut diwujudkan pada konteks spesifik pemrosesan citra, disertai contoh rancangan kontrol, bukti implementasi, dan cara pengujiannya.

Selain kedua standar utama tersebut, pembahasan pada beberapa bagian merujuk pula pada standar dan kerangka pendukung, antara lain panduan manajemen risiko keamanan informasi, panduan penilaian dampak privasi, panduan keamanan layanan awan, serta ketentuan perundang-undangan nasional mengenai perlindungan data pribadi. Rujukan tersebut digunakan sebatas untuk memperjelas konteks penerapan.

G. Tujuan, Ruang Lingkup, dan Sasaran Pembaca Buku

Tujuan buku ini adalah menyediakan kerangka kerja praktis yang dapat digunakan organisasi untuk mengidentifikasi risiko, memilih kontrol, menerapkan pengamanan, serta mengevaluasi efektivitas pengendalian keamanan informasi dan perlindungan data pribadi sepanjang siklus hidup pemrosesan citra.

Untuk mencapai tujuan tersebut, buku ini disusun dengan empat sasaran spesifik. Sasaran pertama adalah membangun pemahaman bersama mengenai anatomi teknis pemrosesan citra sehingga diskusi pengendalian dapat dilakukan pada tingkat kedalaman yang memadai. Sasaran kedua adalah memetakan risiko keamanan dan risiko privasi yang khas pada lingkungan ini. Sasaran ketiga adalah menerjemahkan kontrol standar menjadi rancangan kontrol konkret beserta bukti implementasinya. Sasaran keempat adalah menyediakan instrumen kerja berupa daftar periksa, lembar kerja penilaian, dan templat yang dapat langsung digunakan.

1. Ruang lingkup pembahasan

- a. Citra diam berupa foto dan hasil pindai dokumen
- b. Citra bergerak berupa video, rekaman kamera pengawas, dan siaran langsung
- c. Citra biometrik berupa wajah, iris, sidik jari, dan ciri fisik lain
- d. Citra medis dan citra hasil inspeksi industri
- e. Model kecerdasan buatan yang dilatih menggunakan data citra
- f. Metadata yang menyertai berkas citra

2. Batasan pembahasan

Buku ini tidak membahas rincian algoritma pengolahan citra dari sudut pandang rekayasa, tidak memuat kode program implementasi, dan tidak memberikan pendapat hukum atas kasus tertentu. Pembahasan hukum terbatas pada prinsip yang memengaruhi rancangan kontrol. Nomor klausul dan penomoran kontrol yang disebutkan perlu diverifikasi terhadap edisi standar resmi yang berlaku pada organisasi pembaca.

Tabel 1. 7: Sasaran Pembaca dan Bagian yang Paling Relevan

Kelompok Pembaca	Kebutuhan Utama	Bab yang Disarankan
Praktisi keamanan informasi	Rancangan dan pengujian kontrol	Bab 4, 6, 9, 11
Praktisi privasi dan hukum	Dasar pemrosesan dan hak subjek	Bab 5, 7, 10
Auditor internal dan eksternal	Kriteria audit dan bukti	Bab 6, 9, 12
Pengelola TI dan operasional	Titik kendali pada siklus hidup	Bab 8, 9, 11
Pengembang dan data scientist	Pengamanan model dan data latih	Bab 4, 8, 10
Pengelola CCTV dan analitik video	Penerapan operasional harian	Bab 8, 9, 12
Akademisi dan mahasiswa	Kerangka konseptual menyeluruh	Bab 1 sampai 3, Bab 11

Sumber: Diolah Penulis

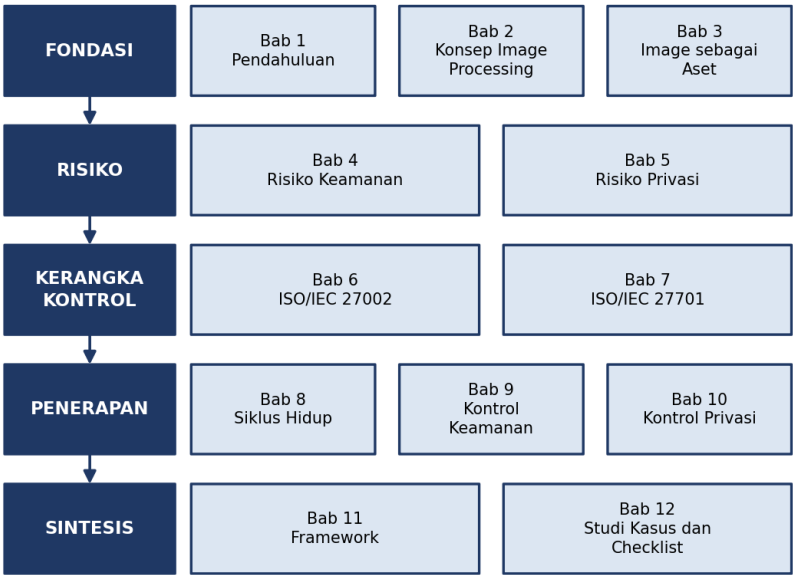
H. Metode dan Struktur Pembahasan Buku

Penyusunan buku ini menggunakan pendekatan yang menggabungkan telaah standar, sintesis praktik, dan penalaran berbasis kasus. Telaah standar dilakukan terhadap maksud dan tujuan kontrol pada ISO/IEC 27002 dan ISO/IEC 27701. Sintesis praktik dilakukan dengan menghimpun pola penerapan yang lazim dijumpai pada organisasi yang mengoperasikan sistem pemrosesan citra. Penalaran berbasis kasus digunakan untuk menguji apakah rancangan kontrol yang diusulkan dapat berjalan pada situasi nyata dengan keterbatasannya.

Struktur pembahasan disusun mengikuti alur berpikir dari fondasi menuju penerapan. Bab 1 sampai Bab 3 membangun fondasi konseptual mengenai teknologi pemrosesan citra dan kedudukan citra sebagai aset informasi. Bab 4 dan Bab 5 membahas lanskap risiko dari dua sudut pandang, yaitu keamanan informasi dan privasi. Bab 6 dan Bab 7 menguraikan kerangka kontrol dari kedua standar rujukan.

Bab 8 sampai Bab 10 merupakan inti penerapan. Bab 8 memetakan siklus hidup pemrosesan citra beserta titik-titik pengendaliannya, Bab 9 memetakan kontrol keamanan informasi ke titik-titik tersebut, dan Bab

10 memetakan kontrol privasi dengan cara yang sama. Bab 11 menyatukan seluruh pembahasan sebelumnya menjadi satu kerangka kerja pengendalian yang utuh, lengkap dengan model kematangan dan indikator kinerja. Bab 12 menutup buku dengan studi kasus, instrumen penilaian mandiri, daftar periksa, dan peta jalan implementasi.



Gambar 1. 1: Struktur Pembahasan Buku

Sumber: Diolah Penulis

Untuk menjaga sifat aplikatif, setiap bab disusun mengikuti pola yang konsisten. Pembahasan dibuka dengan penjelasan konseptual, dilanjutkan dengan penguraian unsur-unsurnya, disertai tabel yang merangkum atau membandingkan, kemudian ditutup dengan contoh penerapan atau matriks kontrol. Tabel dalam buku ini dirancang agar dapat langsung disalin dan disesuaikan oleh pembaca sebagai instrumen kerja, bukan sekadar sebagai ilustrasi.

Pembaca yang menghendaki penerapan cepat dapat memulai dari Bab 12 untuk memperoleh gambaran instrumen yang tersedia, kemudian menelusuri kembali ke bab-bab pemetaan kontrol sesuai kebutuhan. Pembaca yang menghendaki pemahaman menyeluruh disarankan mengikuti urutan bab sebagaimana disusun.

BAB 2

KONSEP DASAR *IMAGE* DAN *VIDEO PROCESSING*

A. Pengertian *Digital Image* dan Video

Citra digital pada hakikatnya adalah representasi numerik dari intensitas cahaya yang tertangkap oleh sensor. Citra disusun sebagai matriks dua dimensi yang setiap elemennya disebut piksel, dan setiap piksel menyimpan nilai intensitas pada rentang tertentu. Pada citra berwarna, setiap piksel menyimpan tiga nilai yang mewakili kanal merah, hijau, dan biru, sehingga citra berwarna sesungguhnya merupakan tiga matriks yang ditumpuk.

Pemahaman bahwa citra adalah kumpulan angka memiliki konsekuensi penting bagi pengendalian keamanan. Karena berupa angka, citra dapat dimodifikasi secara terukur tanpa meninggalkan jejak visual yang kasat mata. Perubahan pada beberapa piksel tertentu dapat menyisipkan informasi tersembunyi, mengubah hasil pengenalan objek, atau menandai berkas tanpa mengubah tampilannya bagi pengamat manusia. Kontrol keutuhan pada citra karenanya tidak dapat bersandar pada pemeriksaan visual.

Video merupakan rangkaian citra yang ditampilkan berurutan dengan laju tertentu, umumnya dinyatakan dalam bingkai per detik. Karakteristik yang membedakan video dari kumpulan foto adalah adanya kompresi antarbingkai. Sebagian besar format video menyimpan hanya satu bingkai kunci secara utuh, kemudian menyimpan bingkai berikutnya sebagai selisih terhadap bingkai sebelumnya. Struktur ini menyebabkan penghapusan sebagian isi video menjadi jauh lebih rumit daripada penghapusan satu foto.

Tabel 2. 1: Parameter Teknis Citra dan Video yang Memengaruhi Pengendalian

Parameter	Penjelasan	Implikasi Pengendalian
Resolusi	Jumlah piksel per bingkai	Menentukan keteridentifikasian wajah
Kedalaman bit	Jumlah tingkat intensitas	Memengaruhi ukuran dan kualitas bukti
Laju bingkai	Bingkai per detik	Menentukan volume penyimpanan
Skema kompresi	Cara pemadatan data	Menyulitkan penghapusan selektif
Ruang warna	Model representasi warna	Memengaruhi akurasi analitik
Kontainer berkas	Format pembungkus	Menentukan kemampuan menyimpan metadata

Sumber: Diolah Penulis

Resolusi merupakan parameter yang paling langsung berkaitan dengan risiko privasi. Kamera dengan resolusi rendah yang hanya mampu menangkap siluet menimbulkan risiko yang berbeda dengan kamera resolusi tinggi yang mampu menangkap ciri wajah secara jelas. Pengendalian resolusi dengan demikian merupakan salah satu bentuk minimalisasi data yang paling efektif dan paling murah, namun jarang dipertimbangkan pada tahap perancangan sistem.

Format berkas juga memiliki implikasi. Format tanpa kompresi mempertahankan seluruh informasi asli sehingga lebih kuat sebagai bukti, tetapi membutuhkan ruang simpan yang besar. Format dengan kompresi *lossy* mengurangi ukuran berkas dengan membuang sebagian informasi yang dianggap tidak signifikan secara visual, namun pembuangan ini dapat menghilangkan detail yang justru penting dalam analisis forensik.

B. Akuisisi dan *Capture Image*

Akuisisi merupakan tahap pertama sekaligus titik kendali paling menentukan dalam keseluruhan siklus hidup pemrosesan citra. Keputusan yang diambil pada tahap ini, seperti apa yang direkam, pada

resolusi berapa, dan dengan sudut pandang seperti apa, menetapkan batas atas dari risiko yang akan ditanggung sepanjang sisa siklus hidup. Data yang tidak pernah dikumpulkan tidak akan pernah bocor.

Proses akuisisi melibatkan sensor yang mengubah cahaya menjadi sinyal listrik, kemudian pengubah analog ke digital yang mengubah sinyal tersebut menjadi nilai numerik. Setelah itu, prosesor sinyal citra pada perangkat melakukan pengolahan awal berupa koreksi warna, pengurangan derau, dan kompresi sebelum berkas dikeluarkan. Sebagian besar perangkat kamera modern menjalankan seluruh rangkaian ini di dalam perangkat itu sendiri.

1. Jenis perangkat akuisisi

- a. Kamera pengawas tetap yang merekam area tertentu secara terus-menerus
- b. Kamera bergerak dengan kemampuan putar, miring, dan perbesaran
- c. Kamera ponsel dan kamera genggam yang digunakan pegawai
- d. Pemindai dokumen dan perangkat pencitraan medis
- e. Kamera pada kendaraan dan wahana udara nirawak
- f. Sensor visual pada lini produksi dan robot industri

2. Aspek pengendalian pada tahap akuisisi

Pengendalian pada tahap akuisisi mencakup penetapan cakupan pandang kamera agar tidak melampaui area yang menjadi tujuan, penetapan resolusi seperlunya, pengaturan waktu operasi, penonaktifan perekaman suara apabila tidak diperlukan, serta pengamanan fisik perangkat agar tidak dapat diarahkan ulang oleh pihak tidak berwenang. Aspek terakhir sering diabaikan padahal perubahan arah kamera merupakan cara termudah untuk memperluas cakupan pengawasan tanpa perubahan konfigurasi apa pun.

Tabel 2. 2: Keputusan Akuisisi dan Dampaknya terhadap Risiko

Keputusan	Pilihan Berisiko Tinggi	Pilihan Berisiko Rendah
Cakupan pandang	Mencakup area publik dan tetangga	Terbatas pada area milik sendiri
Resolusi	Maksimum perangkat	Cukup untuk tujuan yang ditetapkan

Keputusan	Pilihan Berisiko Tinggi	Pilihan Berisiko Rendah
Perekaman suara	Aktif secara bawaan	Nonaktif kecuali diperlukan
Waktu operasi	Dua puluh empat jam penuh	Sesuai jam operasional
Penyimpanan lokal	Kartu memori tanpa enkripsi	Terenkripsi atau langsung dikirim
Kredensial perangkat	Bawaan pabrik	Diubah dan dikelola terpusat

Sumber: Diolah Penulis

Titik lemah yang paling sering ditemukan pada tahap akuisisi adalah kredensial bawaan pabrik yang tidak pernah diubah. Basis data kredensial bawaan berbagai merek kamera tersedia secara terbuka, dan mesin pencari khusus perangkat terhubung internet memungkinkan siapa pun menemukan kamera yang dapat diakses tanpa upaya teknis berarti. Pengubahan kredensial dan penempatan kamera pada segmen jaringan tersendiri merupakan dua kontrol paling mendasar yang harus dipastikan sejak pemasangan.

C. *Pre-processing dan Enhancement*

Tahap prapemrosesan bertujuan menyiapkan citra agar dapat dianalisis dengan hasil yang lebih andal. Operasi yang lazim dilakukan meliputi penyesuaian kecerahan dan kontras, pengurangan derau, penajaman tepi, koreksi distorsi lensa, penyeragaman ukuran, serta normalisasi nilai piksel. Pada sistem pengenalan wajah, tahap ini juga mencakup pelurusan wajah dan penyeragaman pencahayaan.

Dari sudut pandang pengendalian, tahap prapemrosesan memiliki dua implikasi yang berlawanan arah. Implikasi pertama bersifat menguntungkan, karena tahap ini merupakan tempat yang tepat untuk menyisipkan operasi minimalisasi data seperti pengaburan area yang tidak relevan atau pemotongan bagian citra yang berada di luar cakupan tujuan. Menempatkan pengaburan pada tahap ini jauh lebih efektif daripada menerapkannya pada tahap penyajian, karena data yang telanjur tersimpan utuh tetap berisiko.

Implikasi kedua bersifat merugikan, karena setiap operasi prapemrosesan mengubah nilai piksel citra asli. Perubahan ini dapat mengurangi nilai pembuktian citra apabila tidak terdokumentasi. Organisasi yang menggunakan citra sebagai bukti perlu memastikan bahwa citra asli disimpan secara terpisah dan tidak diubah, sementara operasi perbaikan dilakukan pada salinan kerja dengan catatan riwayat operasi yang lengkap.

Tabel 2. 3: Operasi Prapemrosesan dan Pertimbangan Pengendaliannya

Operasi	Tujuan Teknis	Pertimbangan Pengendalian
Pengurangan derau	Memperjelas objek	Dapat menghilangkan detail bukti
Penyesuaian kontras	Memperjelas batas objek	Perlu dicatat pada riwayat
Pemotongan area	Membatasi wilayah analisis	Bentuk minimalisasi yang efektif
Pengaburan area	Menutup area sensitif	Harus tidak dapat dibalik
Penyeragaman ukuran	Menyesuaikan masukan model	Menurunkan keteridentifikasian
Normalisasi warna	Menstabilkan akurasi	Netral terhadap privasi

Sumber: Diolah Penulis

Perlu diperhatikan bahwa tidak semua teknik pengaburan bersifat permanen. Pengaburan yang diterapkan sebagai lapisan tampilan pada perangkat lunak pemutar dapat dilepas dengan mudah, dan pengaburan berbasis pikselasi ringan pada resolusi tinggi dapat dipulihkan sebagian melalui teknik rekonstruksi. Pembahasan mengenai pemilihan teknik pengaburan yang memadai disajikan secara khusus pada subbab 10.6.

D. Segmentation, Feature Extraction, dan Classification

Setelah citra disiapkan, tahap analisis dimulai dengan segmentasi, yaitu pemisahan citra menjadi wilayah-wilayah yang bermakna. Segmentasi memisahkan objek dari latar belakang, misalnya memisahkan sosok

manusia dari pemandangan jalan, atau memisahkan jaringan tertentu dari citra medis. Hasil segmentasi menentukan bagian citra mana yang akan dianalisis lebih lanjut.

Tahap berikutnya adalah ekstraksi fitur, yaitu penghitungan besaran numerik yang merepresentasikan karakteristik objek. Fitur dapat berupa besaran sederhana seperti tepi, sudut, tekstur, dan histogram warna, atau berupa representasi berdimensi tinggi yang dihasilkan oleh lapisan-lapisan jaringan saraf tiruan. Representasi terakhir inilah yang dikenal sebagai vektor fitur atau embedding.

Vektor fitur menempati posisi khusus dalam pembahasan perlindungan data pribadi. Vektor fitur wajah bukan merupakan gambar, tidak dapat dilihat sebagai gambar, dan sering dianggap sebagai data teknis yang tidak sensitif. Anggapan tersebut keliru. Vektor fitur wajah merupakan representasi biometrik yang memungkinkan pencocokan identitas, dapat digunakan untuk menelusuri seseorang di berbagai sistem, dan pada tingkat tertentu dapat direkonstruksi kembali menjadi wajah yang menyerupai aslinya. Vektor fitur karenanya harus diperlakukan sebagai data biometrik dengan tingkat perlindungan yang setara dengan citra wajah aslinya.

Tahap terakhir adalah klasifikasi, yaitu penetapan label terhadap objek berdasarkan fitur yang telah diekstraksi. Klasifikasi menghasilkan keluaran berupa kategori beserta tingkat keyakinan. Keluaran ini bersifat probabilistik, bukan deterministik, dan inilah sumber risiko yang sering diabaikan. Sistem klasifikasi selalu memiliki kemungkinan salah, baik berupa positif palsu maupun negatif palsu, dan konsekuensi kedua jenis kesalahan tersebut berbeda tergantung konteks penggunaannya.

Tabel 2. 4: Keluaran Setiap Tahap Analisis dan Klasifikasi Sensitivitasnya

Tahap	Keluaran	Tingkat Sensitivitas
Segmentasi	Peta wilayah objek	Rendah sampai sedang
Ekstraksi fitur umum	Deskriptor tepi dan tekstur	Rendah
Ekstraksi fitur wajah	Vektor biometrik	Sangat tinggi
Klasifikasi objek	Label dan skor keyakinan	Sedang
Klasifikasi identitas	Identitas individu	Sangat tinggi

Tahap	Keluaran	Tingkat Sensitivitas
Atribut turunan	Perkiraan usia dan jenis kelamin	Tinggi

Sumber: Diolah Penulis

Atribut turunan memerlukan perhatian tersendiri. Sistem yang menyimpulkan usia, jenis kelamin, suasana hati, atau bahkan asal etnis dari citra wajah menghasilkan data pribadi baru yang tidak pernah diberikan oleh subjek data. Pemrosesan semacam ini menciptakan kewajiban perlindungan yang sepenuhnya baru dan pada banyak yurisdiksi memerlukan dasar pemrosesan yang khusus.

E. Object Detection dan Recognition

Deteksi objek merupakan proses menemukan keberadaan dan posisi objek tertentu dalam citra, dinyatakan dalam bentuk kotak pembatas beserta label kelas. Pengenalan objek melangkah lebih jauh dengan menentukan identitas spesifik dari objek yang telah terdeteksi. Perbedaan antara keduanya tampak sederhana namun memiliki implikasi privasi yang sangat berbeda.

Deteksi yang hanya menyatakan bahwa terdapat seseorang pada suatu titik dalam bingkai menghasilkan informasi yang relatif tidak mengidentifikasi. Pengenalan yang menyatakan bahwa orang tersebut adalah individu tertentu menghasilkan data pribadi yang lengkap. Banyak kebutuhan operasional sebenarnya cukup dipenuhi oleh deteksi saja, misalnya penghitungan jumlah pengunjung, pemantauan kepadatan antrean, atau deteksi keberadaan orang pada area terlarang. Penggunaan pengenalan identitas pada kasus semacam ini merupakan pemrosesan berlebihan.

Tabel 2. 5: Tingkatan Analisis Objek dan Kebutuhan Data Pribadi

Tingkat Analisis	Contoh Kebutuhan	Data Pribadi yang Diproses
Deteksi keberadaan	Menghitung jumlah orang	Tidak ada identitas
Deteksi atribut objek	Mendeteksi penggunaan helm	Tidak ada identitas

Tingkat Analisis	Contoh Kebutuhan	Data Pribadi yang Diproses
Pelacakan antarbingkai	Mengukur waktu tunggu	Identitas semu sementara
Pengenalan ulang	Melacak lintas kamera	Identitas semu persisten
Pengenalan identitas	Verifikasi karyawan	Identitas penuh

Sumber: Diolah Penulis

Pelacakan antarbingkai dan pengenalan ulang lintas kamera berada pada wilayah abu-abu yang sering disalahpahami. Kedua teknik tersebut tidak menghasilkan nama, tetapi menghasilkan pengenalan semu yang memungkinkan seorang individu diikuti pergerakannya. Kemampuan mengikuti pergerakan seseorang merupakan bentuk pemrosesan data pribadi meskipun nama individu tersebut tidak pernah diketahui sistem. Prinsip ini penting untuk dipahami karena banyak penyedia solusi memasarkan kemampuan pengenalan ulang sebagai fitur yang tidak berdampak pada privasi.

Dari sudut pandang keamanan informasi, sistem deteksi dan pengenalan menghadapi risiko kekeliruan yang dapat dieksploitasi. Objek dapat dirancang sedemikian rupa agar tidak terdeteksi, atau sebaliknya agar terdeteksi sebagai objek lain. Kerentanan ini dibahas lebih lanjut pada subbab 4.7 mengenai risiko model kecerdasan buatan dan citra adversarial.

F. Facial Recognition dan Biometric Processing

Pengenalan wajah merupakan penerapan pemrosesan citra yang paling banyak menarik perhatian pengatur kebijakan di berbagai negara. Alasannya terletak pada gabungan tiga sifat, yaitu dapat dilakukan dari jarak jauh, tidak memerlukan kerja sama subjek, dan menggunakan ciri yang tidak dapat diganti.

Secara teknis, sistem pengenalan wajah bekerja melalui empat tahap. Tahap pertama adalah deteksi wajah dalam bingkai. Tahap kedua adalah penyesuaian, yaitu penyesuaian posisi dan sudut wajah ke bentuk baku. Tahap ketiga adalah ekstraksi templat berupa vektor numerik. Tahap keempat adalah pencocokan templat dengan basis data templat yang telah tersimpan.

Dua mode operasi perlu dibedakan secara tegas karena tingkat risikonya berbeda jauh. Verifikasi merupakan pencocokan satu banding satu, yaitu memastikan bahwa seseorang adalah orang yang diklaimnya. Identifikasi merupakan pencocokan satu banding banyak, yaitu mencari identitas seseorang dari keseluruhan basis data. Identifikasi memerlukan penyimpanan templat seluruh populasi yang mungkin dikenali, sehingga menciptakan basis data biometrik terpusat yang menjadi sasaran bernilai tinggi bagi penyerang.

Tabel 2. 6: Perbandingan Mode Verifikasi dan Identifikasi Biometrik

Aspek	Verifikasi Satu Banding Satu	Identifikasi Satu Banding Banyak
Pertanyaan yang dijawab	Benarkah ini orang tersebut	Siapakah orang ini
Basis data template	Satu templat per pengguna	Seluruh populasi terdaftar
Kerja sama subjek	Diperlukan	Tidak diperlukan
Risiko kebocoran	Terbatas per pengguna	Massal
Tingkat positif palsu	Rendah	Meningkat seiring ukuran basis data
Alternatif penyimpanan	Templat di perangkat pengguna	Sulit didesentralisasi

Sumber: Diolah Penulis

Penyimpanan templat pada perangkat pengguna merupakan pilihan rancangan yang secara signifikan menurunkan risiko. Pada pola ini, templat tidak pernah meninggalkan perangkat dan pencocokan dilakukan secara lokal, sehingga tidak terbentuk basis data biometrik terpusat. Pola ini dapat diterapkan pada kasus verifikasi, namun tidak dapat diterapkan pada kasus identifikasi. Organisasi yang mempertimbangkan penerapan biometrik perlu memastikan terlebih dahulu apakah kebutuhannya benar-benar memerlukan identifikasi atau cukup dipenuhi dengan verifikasi.

Aspek lain yang perlu diperhatikan adalah ketahanan terhadap pemalsuan. Sistem yang tidak dilengkapi deteksi keaslian dapat ditipu menggunakan foto cetak, tayangan pada layar, atau topeng. Deteksi keaslian merupakan kontrol keamanan yang wajib pada penggunaan

biometrik untuk pengendalian akses, dan ketiadaannya menjadikan seluruh mekanisme autentikasi tidak bermakna.

G. Video Analytics dan CCTV Intelligence

Analitik video merupakan penerapan algoritma pemrosesan citra terhadap aliran video secara berkelanjutan untuk menghasilkan peringatan atau ringkasan otomatis. Sistem ini mengubah kamera pengawas dari perangkat perekam pasif menjadi sensor yang aktif menghasilkan peristiwa.

Kemampuan analitik yang umum:

- 1. Deteksi pelanggaran garis batas dan area terlarang
- 2. Deteksi objek tertinggal atau objek yang hilang
- 3. Penghitungan jumlah orang dan pengukuran kepadatan
- 4. Deteksi perilaku tidak lazim seperti berlari atau berkerumun
- 5. Pembacaan plat nomor kendaraan secara otomatis
- 6. Pencarian cepat berdasarkan ciri seperti warna pakaian

Kemampuan pencarian berdasarkan ciri merupakan perubahan yang paling mengubah lanskap risiko. Pada sistem konvensional, menemukan rekaman seseorang di antara ribuan jam rekaman memerlukan waktu berhari-hari sehingga secara praktis membatasi penyalahgunaan. Pada sistem yang dilengkapi pencarian berbasis ciri, pencarian yang sama selesai dalam hitungan detik. Hambatan praktis yang selama ini berfungsi sebagai pelindung tidak lagi ada, sehingga pengendalian harus digantikan oleh kontrol yang bersifat eksplisit berupa otorisasi dan pencatatan setiap pencarian.

Tabel 2. 7: Perubahan Risiko akibat Penerapan Analitik Video

Aspek	Sebelum Analitik	Setelah Analitik
Waktu pencarian	Berhari-hari	Hitungan detik
Pembatas penyalahgunaan	Kesulitan praktis	Hanya kontrol formal
Data yang dihasilkan	Rekaman mentah	Metadata perilaku
Retensi efektif	Terbatas kapasitas simpan	Metadata bertahan lebih lama
Kebutuhan kontrol	Akses ke ruang kendali	Otorisasi tiap kueri

Sumber: Diolah Penulis

Metadata perilaku yang dihasilkan analitik video sering luput dari kebijakan retensi. Organisasi menetapkan bahwa rekaman video dihapus setelah tiga puluh hari, namun catatan peristiwa hasil analitik yang memuat waktu, lokasi, dan ciri individu tetap tersimpan bertahun-tahun dalam basis data terpisah. Kebijakan retensi yang utuh harus mencakup seluruh turunan data, bukan hanya berkas video.

Aspek ketersediaan juga penting. Sistem analitik yang gagal beroperasi tanpa terdeteksi menciptakan rasa aman yang keliru, karena organisasi meyakini area tertentu terpantau padahal tidak. Pemantauan kesehatan sistem analitik, termasuk deteksi kamera yang tidak mengirim aliran data dan deteksi penurunan mutu gambar, merupakan bagian dari kontrol ketersediaan yang harus dirancang secara eksplisit.

H. *Computer Vision dan Artificial Intelligence*

Perkembangan pembelajaran mendalam telah mengubah cara sistem penglihatan komputer dibangun. Pada pendekatan klasik, fitur dirancang secara manual oleh pengembang berdasarkan pengetahuan domain. Pada pendekatan berbasis pembelajaran mendalam, fitur dipelajari sendiri oleh model dari data pelatihan dalam jumlah besar. Pergeseran ini meningkatkan akurasi secara dramatis namun memindahkan sumber risiko dari kode program ke data.

Model penglihatan komputer terdiri atas beberapa komponen yang masing-masing merupakan aset yang perlu dilindungi. Komponen tersebut meliputi himpunan data pelatihan, arsitektur model, bobot hasil pelatihan, konfigurasi hiperparameter, serta antarmuka inferensi yang melayani permintaan. Kehilangan atau kerusakan pada salah satu komponen berdampak berbeda dan menuntut kontrol yang berbeda pula.

Tabel 2. 8: Komponen Sistem Kecerdasan Buatan Berbasis Citra sebagai Aset

Komponen	Nilai bagi Organisasi	Risiko Utama
Himpunan data pelatihan	Investasi pengumpulan besar	Memuat data pribadi

Komponen	Nilai bagi Organisasi	Risiko Utama
Label dan anotasi	Hasil kerja manual mahal	Kebocoran dan perusakan
Bobot model	Kekayaan intelektual	Pencurian dan ekstraksi
Antarmuka inferensi	Titik layanan operasional	Penyalahgunaan dan kelebihan beban
Catatan permintaan	Bahan peningkatan model	Akumulasi data pribadi

Sumber: Diolah Penulis

Himpunan data pelatihan memerlukan perhatian khusus karena hampir selalu memuat citra individu nyata. Organisasi yang melatih model pengenalan wajah menggunakan rekaman kamera operasionalnya sendiri melakukan penggunaan sekunder atas data yang dikumpulkan untuk tujuan berbeda. Praktik ini memerlukan dasar pemrosesan tersendiri dan pada banyak kerangka regulasi tidak dapat dibenarkan hanya dengan alasan peningkatan mutu layanan.

Model yang telah dilatih juga dapat membocorkan informasi mengenai data pelatihannya. Serangan penentuan keanggotaan memungkinkan penyerang menyimpulkan apakah citra seseorang termasuk dalam data pelatihan, dan serangan inversi model dapat merekonstruksi citra yang menyerupai data pelatihan. Kedua serangan tersebut berarti bahwa penghapusan berkas citra asli tidak otomatis menghapus jejak individu tersebut dari sistem apabila model yang dilatih dengannya masih beroperasi.

I. Metadata, EXIF, Geolocation, dan Informasi Tersembunyi

Setiap berkas citra digital membawa lapisan informasi yang tidak tampak pada gambarnya. Lapisan ini disebut metadata dan pada umumnya jauh lebih kaya daripada yang disadari pengguna. Standar metadata yang paling luas digunakan pada citra diam adalah format pertukaran berkas citra yang lazim disingkat EXIF.

Tabel 2. 9: Kategori Metadata pada Berkas Citra dan Potensi Risikonya

Kategori Metadata	Contoh Isi	Potensi Pengungkapan
Perangkat	Merek, model, nomor seri	Penelusuran ke pemilik perangkat
Waktu	Tanggal dan jam pengambilan	Rekonstruksi kronologi kegiatan
Lokasi	Koordinat lintang dan bujur	Pola pergerakan dan tempat tinggal
Pengaturan optik	Bukaan, kecepatan, ISO	Verifikasi keaslian citra
Pengarang	Nama pembuat dan hak cipta	Identitas pengambil gambar
Riwayat penyuntingan	Perangkat lunak yang dipakai	Indikasi manipulasi
Miniatur tertanam	Salinan kecil citra asli	Menampilkan bagian yang telah disunting

Sumber: Diolah Penulis

Miniatur tertanam merupakan risiko yang paling sering terlewat. Ketika sebuah citra disunting untuk menutupi bagian tertentu, sebagian perangkat lunak tidak memperbarui miniatur yang tertanam di dalam metadata. Akibatnya, berkas hasil suntingan masih menyimpan versi kecil dari citra asli yang belum ditutupi, dan versi tersebut dapat diekstraksi dengan mudah menggunakan perangkat baca metadata standar.

Informasi lokasi juga menuntut kehati-hatian tinggi. Kumpulan foto yang diunggah pegawai ke saluran internal maupun eksternal dapat mengungkap lokasi fasilitas yang seharusnya tidak dipublikasikan, pola perjalanan personel tertentu, atau alamat tempat tinggal. Kebijakan penghapusan metadata sebelum publikasi merupakan kontrol sederhana dengan dampak perlindungan yang besar.

Selain metadata baku, citra dapat memuat informasi yang sengaja disembunyikan melalui teknik steganografi. Teknik ini menyisipkan data ke dalam nilai piksel sedemikian rupa sehingga tidak terdeteksi secara visual. Dari sudut pandang keamanan, kanal semacam ini dapat dimanfaatkan untuk pengeluaran data secara diam-diam maupun untuk penyaluran perintah kepada perangkat lunak berbahaya. Organisasi

dengan tingkat kerahasiaan tinggi perlu mempertimbangkan penerapan normalisasi ulang citra pada gerbang keluar untuk merusak kanal tersembunyi tersebut.

J. Arsitektur Sistem *Image processing: Edge, Server, Cloud,* dan AI

Pemilihan arsitektur menentukan di mana citra berada, siapa yang dapat mengaksesnya, dan kontrol apa yang secara teknis mungkin diterapkan. Terdapat tiga pola arsitektur utama beserta bentuk campurannya, dan masing-masing memiliki profil risiko yang khas.

1. Pemrosesan di tepi

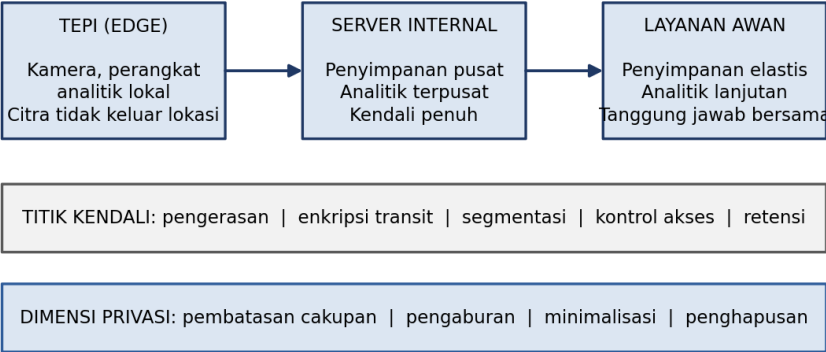
Pada pola ini, analisis dilakukan pada perangkat di lokasi akuisisi, dan hanya hasil analisis yang dikirim ke pusat. Keunggulannya adalah citra mentah tidak pernah meninggalkan lokasi sehingga permukaan risiko privasi jauh lebih kecil. Kelemahannya adalah perangkat tepi tersebar secara fisik, sulit diperbarui secara serempak, dan memiliki kapasitas komputasi terbatas.

2. Pemrosesan pada server internal

Pada pola ini, aliran citra dikirim ke pusat data organisasi untuk disimpan dan dianalisis. Keunggulannya adalah kendali penuh berada di tangan organisasi dan kontrol dapat diterapkan secara terpusat. Kelemahannya adalah terbentuknya penyimpanan terpusat yang menjadi sasaran bernilai tinggi, serta beban jaringan yang besar untuk mengangkut aliran video dari seluruh titik.

3. Pemrosesan pada layanan awan

Pada pola ini, penyimpanan dan analisis diserahkan kepada penyedia layanan awan. Keunggulannya adalah skalabilitas dan ketersediaan kemampuan analitik mutakhir tanpa investasi perangkat keras. Kelemahannya adalah citra keluar dari batas kendali organisasi, tunduk pada model tanggung jawab bersama, dan berpotensi berpindah lintas wilayah hukum.



Gambar 2. 1 Pola Arsitektur Sistem Pemrosesan Citra

Sumber: Diolah Penulis

Tabel 2. 10: Perbandingan Profil Risiko Tiga Pola Arsitektur

Aspek	Tepi	Server Internal	Awan
Lokasi citra mentah	Perangkat lokal	Pusat data organisasi	Infrastruktur penyedia
Permukaan serangan	Tersebar luas	Terpusat	Bergantung penyedia
Kemudahan pembaruan	Rendah	Tinggi	Sangat tinggi
Kendali kunci enkripsi	Terbatas	Penuh	Perlu diperjanjikan
Risiko lintas batas	Tidak ada	Tidak ada	Perlu dikaji
Kemampuan analitik	Terbatas	Sedang	Tinggi

Sumber: Diolah Penulis

Dalam praktik, sebagian besar organisasi menerapkan pola campuran. Pola yang secara umum paling menguntungkan dari sudut pandang perlindungan adalah melakukan deteksi dan pengaburan pada

tepi, mengirim hanya citra yang telah diminimalkan ke *server* internal untuk penyimpanan, dan menggunakan layanan awan hanya untuk beban analitik yang tidak memerlukan citra mentah. Rancangan semacam ini mewujudkan prinsip privasi sejak perancangan pada tingkat arsitektur, bukan hanya pada tingkat kebijakan.

BAB 3

IMAGE SEBAGAI ASET

INFORMASI

A. Konsep Aset Informasi

Aset informasi dipahami sebagai segala sesuatu yang memiliki nilai bagi organisasi dan berkaitan dengan informasi. Cakupannya tidak terbatas pada data itu sendiri, melainkan juga meliputi media penyimpanan, perangkat pengolah, perangkat lunak, layanan pendukung, dan pengetahuan yang melekat pada personel. Pemahaman yang luas ini penting karena perlindungan terhadap data tidak akan efektif apabila perangkat dan layanan yang mengolahnya tidak turut dilindungi.

Pada lingkungan pemrosesan citra, batas aset menjadi lebih kabur dibandingkan lingkungan sistem informasi konvensional. Sebuah kamera merupakan perangkat sekaligus penghasil data sekaligus penyimpan sementara. Sebuah model kecerdasan buatan merupakan perangkat lunak sekaligus representasi terkompresi dari data pelatihannya. Ketidakjelasan batas ini menyebabkan banyak organisasi gagal mencatat sebagian aset dalam inventarisnya.

Prinsip yang digunakan dalam buku ini adalah bahwa segala sesuatu yang dapat menyebabkan citra terungkap, berubah, atau tidak tersedia merupakan bagian dari lingkup aset yang harus dikelola. Prinsip ini menghasilkan cakupan inventaris yang lebih luas daripada praktik umum, namun justru mencerminkan permukaan risiko yang sebenarnya.

BAB 4

RISIKO KEAMANAN

INFORMASI PADA *IMAGE*

PROCESSING

A. Konsep *Threat, Vulnerability, Likelihood, dan Impact*

Risiko keamanan informasi lahir dari pertemuan antara ancaman, kerentanan, dan aset yang bernilai. Ancaman merupakan potensi penyebab kejadian yang tidak diinginkan, kerentanan merupakan kelemahan yang dapat dimanfaatkan oleh ancaman, dan aset merupakan sesuatu yang bernilai sehingga kerusakannya menimbulkan kerugian. Ketiadaan salah satu unsur meniadakan risiko.

Pemahaman atas hubungan ketiga unsur tersebut memiliki konsekuensi praktis dalam penetapan kontrol. Kontrol dapat diarahkan untuk mengurangi paparan terhadap ancaman, menutup kerentanan, atau mengurangi nilai yang terpapar. Pada lingkungan pemrosesan citra, opsi terakhir sering merupakan yang paling efektif, namun paling jarang dipertimbangkan, karena mengurangi jumlah dan kualitas citra yang dikumpulkan secara langsung dapat menurunkan nilai yang dapat hilang.

BAB 5

RISIKO PRIVASI DAN PERLINDUNGAN DATA PRIBADI

A. *Image dan Video sebagai Data Pribadi*

Pertanyaan mendasar yang harus dijawab sebelum membahas risiko privasi adalah kapan sebuah citra berkedudukan sebagai data pribadi. Jawaban atas pertanyaan ini menentukan berlaku atau tidaknya seluruh kewajiban perlindungan data pribadi terhadap suatu aliran citra.

Data pribadi dipahami sebagai setiap informasi mengenai orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara tersendiri maupun dikombinasikan dengan informasi lain. Frasa yang dapat diidentifikasi merupakan kunci, karena memperluas cakupan jauh melampaui citra yang menampilkan wajah secara jelas.

Sebuah citra dapat berkedudukan sebagai data pribadi meskipun wajah tidak tampak. Postur tubuh yang khas, cara berjalan, pakaian seragam bernomor, pelat nomor kendaraan, tato, alat bantu jalan, hingga kombinasi antara lokasi dan waktu dapat memungkinkan identifikasi apabila digabungkan dengan informasi lain yang dimiliki organisasi. Sebuah rekaman punggung seseorang yang memasuki ruangan pada pukul tertentu menjadi data pribadi ketika organisasi juga memiliki catatan kehadiran pada waktu yang sama.

BAB 6

KERANGKA KONTROL ISO/IEC 27002 UNTUK *IMAGE* *PROCESSING*

A. Posisi ISO/IEC 27002 dalam Pengendalian Keamanan Informasi

Keluarga standar ISO/IEC 27000 menyediakan kerangka menyeluruh untuk pengelolaan keamanan informasi. Di dalamnya, ISO/IEC 27001 menetapkan persyaratan sistem manajemen yang harus dipenuhi organisasi, sedangkan ISO/IEC 27002 menyediakan panduan penerapan atas kontrol yang dirujuk oleh persyaratan tersebut. Perbedaan ini penting karena menentukan cara kedua dokumen digunakan.

ISO/IEC 27001 bersifat normatif dan menjadi dasar sertifikasi. Organisasi menyatakan pemenuhan terhadapnya dan dapat diaudit oleh lembaga sertifikasi. ISO/IEC 27002 bersifat panduan dan tidak dapat disertifikasi. Fungsinya adalah menjelaskan maksud setiap kontrol, memberikan petunjuk penerapan, serta menyediakan informasi lain yang membantu organisasi merancang kontrol yang sesuai konteksnya.

BAB 7

KERANGKA PRIVASI ISO/IEC 27701 UNTUK *IMAGE* *PROCESSING*

A. *Privacy Information Management dalam Konteks Image Processing*

Sistem manajemen informasi privasi merupakan perluasan dari sistem manajemen keamanan informasi yang menambahkan persyaratan dan panduan khusus untuk perlindungan informasi pribadi. Perluasan ini bekerja dengan cara memperkaya persyaratan yang telah ada dan menambahkan kelompok kontrol baru, bukan dengan membangun sistem yang terpisah.

Pilihan perluasan tersebut memiliki konsekuensi praktis yang penting. Organisasi yang telah menjalankan sistem manajemen keamanan informasi tidak perlu membangun struktur baru, melainkan memperluas cakupan yang telah ada. Kebijakan, penilaian risiko, program audit, dan tinjauan manajemen yang telah berjalan diperluas agar turut mencakup dimensi privasi.

Pada lingkungan pemrosesan citra, integrasi ini sangat menguntungkan karena hampir seluruh aset yang dikelola memiliki kedua dimensi sekaligus. Memisahkan pengelolaan rekaman kamera menjadi dua sistem yang berbeda menghasilkan duplikasi inventaris, duplikasi penilaian risiko, dan pada akhirnya ketidaksesuaian antara keduanya.

BAB 8

SIKLUS HIDUP *IMAGE* *PROCESSING* DAN TITIK PENGENDALIAN

A. *Image Processing Lifecycle*

Siklus hidup pemrosesan citra menggambarkan seluruh tahap yang dilalui citra sejak diciptakan sampai dimusnahkan. Penggunaan siklus hidup sebagai kerangka analisis memberikan tiga keuntungan yang tidak diperoleh dari pendekatan berbasis sistem.

Keuntungan pertama adalah kelengkapan. Pendekatan berbasis sistem cenderung melewati tahap yang berlangsung di antara sistem, seperti perpindahan data dan penyangga sementara, sedangkan pendekatan siklus hidup memaksa seluruh tahap teridentifikasi. Keuntungan kedua adalah ketepatan penempatan kontrol, karena setiap tahap memiliki ancaman yang khas sehingga kontrol dapat ditempatkan pada titik yang paling efektif. Keuntungan ketiga adalah kemudahan penilaian kelengkapan, karena kesenjangan pada satu tahap menjadi mudah terlihat.

BAB 9

PEMETAAN KONTROL KEAMANAN INFORMASI

A. Metodologi *Control Mapping*

Pemetaan kontrol merupakan proses menghubungkan risiko yang telah diidentifikasi dengan kontrol standar, kemudian menerjemahkan kontrol tersebut menjadi rancangan penerapan yang spesifik pada konteks pemrosesan citra. Hasil pemetaan berupa matriks yang dapat digunakan sebagai rencana penerapan sekaligus kriteria audit.

Metodologi yang digunakan dalam bab ini terdiri atas lima langkah. Langkah pertama adalah menetapkan domain kontrol berdasarkan kapabilitas operasional. Langkah kedua adalah mengidentifikasi risiko yang termasuk dalam domain tersebut. Langkah ketiga adalah memilih kontrol standar yang relevan. Langkah keempat adalah merumuskan rancangan penerapan spesifik beserta buktinya. Langkah kelima adalah menetapkan metode pengujian efektivitas.

Tabel 9. 1: Struktur Baku Setiap Entri Pemetaan Kontrol

Unsur	Isi
Domain	Kelompok kapabilitas operasional
Risiko yang ditangani	Kode risiko dari daftar risiko
Kontrol standar	Rujukan tema dan maksud kontrol
Rancangan penerapan	Mekanisme spesifik pada konteks citra
Bukti implementasi	Artefak yang dihasilkan kontrol

BAB 10

PEMETAAN KONTROL PRIVASI

A. Pemetaan PII dalam *Image Processing*

Langkah pertama dalam pemetaan kontrol privasi adalah mengetahui secara tepat informasi pribadi apa saja yang terkandung dalam ekosistem pemrosesan citra. Tanpa pemetaan ini, kontrol diterapkan berdasarkan asumsi dan hampir selalu meninggalkan kategori data yang tidak tersentuh.

Pemetaan dilakukan dengan menelusuri setiap tahap siklus hidup dan mengidentifikasi bentuk informasi pribadi yang muncul pada tahap tersebut. Penelusuran ini mengungkapkan bahwa informasi pribadi tidak hanya berada pada berkas citra, melainkan tersebar pada berbagai bentuk turunan yang sering dikelola oleh sistem berbeda dengan kontrol berbeda.

Tabel 10. 1: Bentuk Informasi Pribadi pada Ekosistem Pemrosesan Citra

Bentuk	Lokasi Tipikal	Sering Terlewat
Berkas citra dan video	Penyimpanan utama	Tidak
Miniatur pratayang	Basis data indeks	Ya
Templat biometrik	Basis data pengenalan	Tidak
Vektor fitur objek	Basis data analitik	Ya
Metadata peristiwa	Basis data peristiwa	Ya
Pengenal pelacakan	Basis data analitik	Ya
Metadata berkas	Melekat pada berkas	Ya

BAB 11

FRAMEWORK PENGENDALIAN KEAMANAN INFORMASI DAN PRIVASI PADA ***IMAGE*** ***PROCESSING***

A. Prinsip dan Tujuan *Framework*

Sepuluh bab sebelumnya telah menguraikan teknologi, aset, risiko, kerangka kontrol, siklus hidup, serta pemetaan kontrol keamanan dan kontrol privasi secara terpisah. Bab ini menyatukan seluruhnya menjadi satu kerangka kerja yang dapat diterapkan sebagai program kerja organisasi.

Kerangka kerja yang disusun bertujuan menjawab empat pertanyaan yang selalu muncul pada penerapan nyata. Pertanyaan pertama adalah dari mana memulai ketika sistem sudah beroperasi selama bertahun-tahun tanpa pengendalian. Pertanyaan kedua adalah bagaimana menentukan urutan penerapan ketika sumber daya terbatas. Pertanyaan ketiga adalah bagaimana mengukur bahwa pengendalian benar-benar bekerja. Pertanyaan keempat adalah bagaimana menjaga agar pengendalian tetap relevan ketika teknologi berubah.

Prinsip yang mendasari kerangka kerja:

1. Berbasis risiko, sehingga tingkat pengendalian sepadan dengan tingkat risiko

BAB 12

STUDI KASUS, *ASSESSMENT*, DAN *CHECKLIST* *IMPLEMENTASI*

A. Studi Kasus CCTV di Area Publik dan Perkantoran

Sebuah perusahaan jasa dengan gedung kantor delapan lantai mengoperasikan seratus dua puluh kamera yang mencakup area lobi, koridor, ruang kerja terbuka, area parkir, dan pintu masuk. Sistem telah beroperasi selama enam tahun dengan penambahan bertahap tanpa dokumentasi terpusat. Rekaman disimpan pada perekam jaringan di ruang teknis dan dapat diakses oleh seluruh petugas keamanan menggunakan satu akun bersama.

1. Temuan penilaian

- a. Tiga puluh dua kamera tidak tercatat dalam dokumen apa pun dan tidak diketahui siapa yang memasangnya
- b. Empat kamera mengarah ke area istirahat dan satu mengarah ke area sanitasi
- c. Kredensial bawaan pabrik masih digunakan pada delapan puluh persen perangkat
- d. Masa simpan ditentukan oleh kapasitas cakram sehingga bervariasi antara empat puluh dan sembilan puluh hari
- e. Tidak terdapat papan pemberitahuan pada tiga dari lima titik masuk
- f. Ekspor rekaman dilakukan melalui penyalinan ke perangkat penyimpanan pribadi petugas
- g. Tidak terdapat catatan mengenai siapa memutar rekaman apa

LAMPIRAN A TEMPLAT ASSET

REGISTER IMAGE/VIDEO

Lampiran ini memuat templat inventaris aset citra dan video sebagaimana diuraikan pada subbab 3.6. Templat diisi pada tingkat aliran citra, yaitu satu entri untuk setiap sumber citra beserta seluruh turunannya. Kolom sistem hilir merupakan kolom yang paling menentukan karena menjadi dasar pemenuhan hak subjek data dan pelaksanaan jadwal retensi.

Tabel L.A. 1: Struktur Kolom Asset *Register Image* dan *Video*

No	Kolom	Panduan Pengisian
1	Kode aliran	Pengenal unik, misalnya CAM-GD1-L02-004
2	Nama aliran	Sebutan operasional yang dikenal pengguna
3	Jenis perangkat	Kamera tetap, bergerak, ponsel, pemindai, medis
4	Lokasi fisik	Gedung, lantai, titik pemasangan
5	Area cakupan	Uraian area yang terekam
6	Tujuan pemrosesan	Alasan sah pengumpulan, dirumuskan spesifik
7	Dasar pemrosesan	Kewajiban hukum, kepentingan sah, perjanjian, persetujuan
8	Kategori subjek data	Pegawai, pelanggan, publik, pasien, anak, vendor
9	Klasifikasi	Publik, internal, terbatas, sangat rahasia
10	Pemilik aset	Unit dan jabatan penanggung jawab keputusan
11	Kustodian	Unit pengelola operasional
12	Resolusi	Parameter resolusi yang ditetapkan
13	Laju bingkai	Bingkai per detik
14	Jadwal perekaman	Rentang jam dan hari operasi
15	Perekaman suara	Aktif atau nonaktif beserta dasarnya
16	Lokasi penyimpanan utama	Sistem dan wilayah geografis
17	Lokasi cadangan	Sistem dan wilayah geografis

No	Kolom	Panduan Pengisian
18	Periode retensi	Masa simpan dan dasar penetapannya
19	Metode penghapusan	Otomatis terjadwal atau manual
20	Sistem hilir	Analitik, model, basis data turunan
21	Data turunan dihasilkan	Templat, vektor fitur, metadata peristiwa
22	Penerima internal	Unit yang berhak mengakses
23	Penerima eksternal	Pihak ketiga dan dasar penyerahannya
24	Pemroses terkait	Vendor dengan perjanjian pemrosesan
25	Penilaian dampak	Nomor dan tanggal laporan penilaian
26	Tanggal pemasangan	Waktu perangkat mulai beroperasi
27	Tanggal peninjauan terakhir	Waktu entri terakhir diverifikasi
28	Status	Aktif, nonaktif, direncanakan dihentikan

Sumber: Diolah Penulis

Pemutakhiran entri dikaitkan dengan proses manajemen perubahan. Setiap pemasangan perangkat baru, perubahan arah kamera, penambahan modul analitik, atau perubahan penyedia penyimpanan memicu pemutakhiran. Rekonsiliasi antara inventaris dan hasil pemeriksaan lapangan dilakukan sekurang-kurangnya setahun sekali.

LAMPIRAN B TEMPLAT *RISK REGISTER*

Lampiran ini memuat templat daftar risiko terpadu sebagaimana diuraikan pada subbab 4.11 dan subbab 11.3, beserta contoh entri yang mencakup risiko keamanan informasi dan risiko privasi pada pemrosesan citra. Contoh entri dapat digunakan sebagai titik awal yang kemudian disesuaikan dengan konteks organisasi.

Tabel L.B. 1: Struktur Kolom *Risk Register* Terpadu

No	Kolom	Panduan Pengisian
1	Kode risiko	Pengenal unik untuk penelusuran
2	Aliran terkait	Rujukan kode aliran pada asset register
3	Skenario risiko	Aset, ancaman, kerentanan, dan akibat
4	Kategori	Keamanan informasi atau privasi
5	Tahap siklus hidup	Tahap tempat risiko terwujud
6	Kontrol yang telah ada	Kontrol berjalan saat penilaian
7	Kemungkinan	Nilai satu sampai lima
8	Dampak organisasi	Nilai satu sampai lima
9	Dampak individu	Nilai satu sampai lima
10	Dampak dipakai	Nilai tertinggi di antara kolom 8 dan 9
11	Nilai risiko awal	Kolom 7 dikalikan kolom 10
12	Tingkat risiko	Rendah, sedang, tinggi, sangat tinggi
13	Opsi penanganan	Mitigasi, hindari, alihkan, terima
14	Kontrol tambahan	Rujukan matriks kontrol
15	Pemilik tindakan	Jabatan penanggung jawab
16	Tenggat	Batas waktu penyelesaian
17	Nilai risiko sisa	Perkiraan setelah kontrol tambahan
18	Status	Rencana, berjalan, selesai, diterima
19	Tanggal peninjauan	Waktu entri terakhir ditinjau

Sumber: Diolah Penulis

Tabel L.B. 2: Contoh Entri *Risk Register* Kategori Keamanan Informasi

Kode	Skenario Ringkas	K	D	Nilai	Kontrol Tambahan
R-01	Kredensial bawaan pabrik pada kamera	4	4	16	Pengerasan, brankas kredensial
R-02	Ekspor rekaman melalui aplikasi pesan pribadi	5	3	15	Kendali ekspor, tanda air, kesadaran
R-03	Akun bersama menghilangkan akuntabilitas	5	3	15	Identitas perseorangan, faktor ganda
R-04	Administrator melihat rekaman tanpa keperluan	3	4	12	Pemisahan tugas, pencatatan alasan
R-05	Monitor pengawasan terlihat dari area publik	3	3	9	Penempatan layar, filter privasi
R-06	Media penyimpanan dicuri dari lokasi kamera	2	4	8	Pengamanan fisik, enkripsi media
R-11	Penyimpanan terenkripsi perangkat pemeras	3	5	15	Cadangan terpisah, pengerasan, deteksi
R-12	Kamera terinfeksi menjadi pijakan masuk	3	4	12	Segmentasi, pembatasan akses keluar
R-13	Perangkat tegar palsu dipasang saat pemeliharaan	2	5	10	Verifikasi tanda tangan, pengawasan vendor
R-16	Aliran kamera tanpa enkripsi disadap	4	4	16	Enkripsi transit, segmentasi
R-20	Antarmuka kamera terekspos ke internet	3	5	15	Peninjauan aturan, pemindaian dari luar
R-25	Model berperilaku bias antarkelompok	4	4	16	Uji kinerja per kelompok, peninjauan manusia
R-26	Operator memantau individu karena kepentingan pribadi	4	4	16	Deteksi pola, peninjauan independen
R-29	Rekaman terkait penyelidikan terhapus otomatis	3	4	12	Penahanan penghapusan, peninjauan daftar
R-30	Personel yang berhenti masih memiliki akses	3	4	12	Integrasi kepegawaian, tinjauan akses

Sumber: Diolah Penulis

Tabel L.B. 3: Contoh Entri Risk Register Kategori Privasi

Kode	Skenario Ringkas	K	D	Nilai	Kontrol Tambahan
P-01	Kamera mencakup area dengan ekspektasi privasi tinggi	3	5	15	Penutupan area, peninjauan cakupan
P-02	Subjek data tidak mengetahui adanya perekaman	4	3	12	Papan pemberitahuan berlapis
P-03	Pemberitahuan tidak menyebutkan adanya analitik	4	3	12	Pemutakhiran isi pemberitahuan
P-04	Biometrik diproses tanpa dasar pemrosesan yang sah	3	5	15	Analisis dasar, alternatif nonbiometrik
P-05	Rekaman digunakan menilai kinerja pegawai	3	4	12	Kebijakan larangan, persetujuan formal
P-06	Retensi tidak ditetapkan sehingga data menumpuk	5	3	15	Jadwal retensi, penghapusan otomatis
P-07	Penghapusan tidak mencakup cadangan dan turunan	4	4	16	Perluasan cakupan, verifikasi berkala
P-08	Permintaan hak subjek tidak dapat dipenuhi	4	3	12	Kemampuan cari dan aburkan, prosedur
P-09	Data mengalir ke pemroses tanpa perjanjian	3	4	12	Perjanjian pemrosesan, penilaian vendor
P-10	Data berpindah lintas wilayah tanpa pengaman	3	4	12	Pembatasan wilayah, mekanisme pengaman
P-11	Model dilatih dengan rekaman tanpa dasar	3	4	12	Analisis dasar, anonimisasi data latih
P-12	Pengenal pelacakan persisten membentuk riwayat	4	4	16	Pembaruan pengenalan berkala
P-13	Citra anak diproses tanpa perlindungan tambahan	2	5	10	Perlakuan khusus, persetujuan wali

Kode	Skenario Ringkas	K	D	Nilai	Kontrol Tambahan
P-14	Rekaman diserahkan tanpa pengaburan pihak lain	4	3	12	Pengaburan selektif pada ekspor
P-15	Fitur analitik aktif tanpa digunakan dan tanpa dasar	4	3	12	Penonaktifan fitur tidak terpakai

Sumber: Diolah Penulis

LAMPIRAN C TEMPLAT

PRIVACY IMPACT ASSESSMENT

Lampiran ini memuat templat penilaian dampak perlindungan data sebagaimana diuraikan pada subbab 5.9. Penilaian dilaksanakan sebelum pemrosesan dimulai, bukan sebagai dokumentasi setelah sistem berjalan.

Tabel L.C. 1: Bagian Satu Identifikasi Kegiatan Pemrosesan

Butir	Isian
Nama kegiatan	Sebutan sistem atau kegiatan yang dinilai
Unit pengusul	Unit yang mengajukan kegiatan
Tanggal penilaian	Waktu pelaksanaan penilaian
Pelaksana penilaian	Nama dan jabatan tim penilai
Uraian kegiatan	Penjelasan alur pemrosesan secara menyeluruh
Tujuan pemrosesan	Rumusan tujuan yang spesifik dan tegas
Dasar pemrosesan	Dasar hukum yang digunakan
Kategori data	Jenis informasi pribadi yang diproses
Kategori subjek data	Kelompok individu yang terdampak
Perkiraan jumlah subjek	Estimasi individu yang terdampak
Teknologi yang digunakan	Perangkat, algoritma, dan penyedia
Penerima data	Pihak internal dan eksternal
Perpindahan lintas wilayah	Wilayah tujuan dan mekanisme pengaman
Masa simpan	Periode retensi dan dasarnya

Sumber: Diolah Penulis

Tabel L.C. 2: Bagian Dua Uji Kebutuhan dan Proporsionalitas

Pertanyaan	Panduan Penilaian
Apakah tujuan sah dan spesifik	Tujuan tidak boleh dirumuskan terlalu umum
Apakah pemrosesan diperlukan untuk tujuan tersebut	Buktikan keterkaitan langsung

Pertanyaan	Panduan Penilaian
Apakah terdapat alternatif yang kurang mengganggu	Uraikan alternatif dan alasan tidak dipilih
Apakah lingkup data telah diminimalkan	Uraikan penerapan minimalisasi
Apakah masa simpan telah diminimalkan	Uraikan dasar penetapan periode
Apakah manfaat sepadan dengan gangguan	Uraikan penyeimbangan kepentingan
Apakah subjek data memperoleh informasi	Uraikan mekanisme pemberitahuan
Apakah hak subjek data dapat dipenuhi	Uraikan kemampuan teknis yang tersedia

Sumber: Diolah Penulis

Tabel L.C. 3: Bagian Tiga Identifikasi dan Penilaian Risiko terhadap Individu

Kolom	Panduan Pengisian
Risiko terhadap individu	Uraikan kerugian yang mungkin dialami
Sumber risiko	Tahap dan penyebab timbulnya risiko
Kemungkinan	Nilai satu sampai lima
Keparahan bagi individu	Nilai satu sampai lima
Nilai risiko	Hasil perkalian kedua nilai
Tindakan mitigasi	Kontrol yang akan diterapkan
Risiko sisa	Perkiraan setelah mitigasi
Dapat diterima	Ya atau tidak beserta alasan

Tabel L.C. 4: Bagian Empat Kesimpulan dan Persetujuan

Butir	Isian
Ringkasan risiko sisa	Gambaran risiko setelah mitigasi
Rekomendasi	Lanjut, lanjut bersyarat, atau tidak lanjut
Syarat yang harus dipenuhi	Daftar prasyarat sebelum penerapan
Pendapat petugas perlindungan data	Pandangan tertulis
Konsultasi pemangku kepentingan	Pihak yang dilibatkan dan masukannya

Butir	Isian
Keputusan pimpinan	Persetujuan atau penolakan
Tanggal peninjauan berikutnya	Jadwal pemutakhiran penilaian

Sumber: Diolah Penulis

LAMPIRAN D TEMPLAT

CONTROL MAPPING ISO/IEC

27002

Lampiran ini memuat matriks pemetaan kontrol keamanan informasi sebagaimana diuraikan pada Bab 6 dan Bab 9. Kolom status penerapan, pemilik kontrol, dan tanggal pengujian terakhir ditambahkan agar matriks berfungsi sebagai alat kendali yang hidup.

Tabel L.D. 1: Struktur Kolom *Control Mapping*

Kolom	Panduan Pengisian
Kode kontrol	Pengenal internal untuk penelusuran
Domain	Kelompok kapabilitas operasional
Tema kontrol	Organisasional, orang, fisik, teknologi
Maksud kontrol	Hasil yang hendak dicapai
Risiko yang ditangani	Kode risiko dari risk register
Tahap siklus hidup	Tahap tempat kontrol diterapkan
Rancangan penerapan	Mekanisme spesifik pada konteks citra
Bukti implementasi	Artefak yang dihasilkan kontrol
Metode uji	Cara memverifikasi efektivitas
Indikator kegagalan	Tanda kontrol tidak bekerja
Pemilik kontrol	Jabatan penanggung jawab
Status penerapan	Belum, sebagian, penuh
Tanggal uji terakhir	Waktu pengujian efektivitas
Hasil uji	Efektif, efektif dengan pengecualian, tidak efektif

Sumber: Diolah Penulis

Tabel L.D. 2: Matriks *Control Mapping Domain* Tata Kelola dan Aset

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Kebijakan pengawasan visual	Kebijakan khusus disahkan dan disosialisasikan	Dokumen dan bukti sosialisasi	Telaah dokumen dan wawancara
Peran dan tanggung jawab	Pemilik ditetapkan untuk setiap aliran	Matriks peran	Uji sampel aliran
Pemisahan tugas	Operator terpisah dari pengelola catatan	Bagan wewenang dan konfigurasi	Uji kewenangan akun
Inventaris aset	Seluruh aliran dan turunan tercatat	Berkas inventaris	Rekonsiliasi lapangan
Klasifikasi informasi	Setiap aliran memiliki tingkat sensitivitas	Kolom klasifikasi	Uji sampel kesesuaian
Pengelolaan pemasok	Klausul keamanan pada kontrak vendor	Kontrak dan penilaian vendor	Telaah kontrak
Kepatuhan hukum	Daftar kewajiban dan pemetaannya	Daftar kewajiban	Telaah kemutakhiran
Kesinambungan usaha	Rencana pemulihan sistem pengawasan	Rencana dan hasil uji	Telaah hasil latihan

Sumber: Diolah Penulis

Tabel L.D. 3: Matriks *Control Mapping Domain* Teknologi

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Identitas perseorangan	Akun per pengguna tanpa akun bersama	Daftar akun aktif	Telaah akun generik
Hak akses berbasis peran	Akses per kamera, fungsi, dan rentang waktu	Matriks hak akses	Uji sampel akun
Peninjauan akses berkala	Tinjauan triwulanan oleh pemilik aset	Kertas kerja tinjauan	Telaah bukti tinjauan

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Autentikasi berfaktor ganda	Wajib untuk pemutaran, pencarian, ekspor	Konfigurasi sistem	Uji percobaan akses
Pengelolaan kredensial perangkat	Kata sandi unik per kamera dari brankas	Catatan brankas	Uji sampel kredensial
Enkripsi transit	Aliran dan sesi terenkripsi	Konfigurasi dan hasil tangkap	Pemeriksaan teknis
Enkripsi penyimpanan	Volume rekaman terenkripsi	Konfigurasi penyimpanan	Verifikasi status
Pemisahan kunci	Kunci pada sistem pengelola terpisah	Arsitektur kunci	Telaah lokasi kunci
Segmentasi jaringan	Kamera pada segmen terpisah	Diagram dan konfigurasi	Uji jangkauan antarsegmen
Pembatasan akses keluar	Kamera tidak dapat menghubungi internet	Aturan penyaringan	Uji koneksi keluar
Pengerasan perangkat	Layanan tidak perlu dimatikan	Baku konfigurasi dan pindai	Pindai sampel
Pengelolaan perangkat tegar	Pembaruan terjadwal dan tercatat	Catatan versi	Telaah versi terpasang
Kelengkapan pencatatan	Seluruh peristiwa wajib tercatat	Contoh catatan	Uji tindakan dan cek catatan
Perlindungan catatan	Catatan dikirim ke sistem terpisah	Arsitektur pencatatan	Uji percobaan penghapusan
Deteksi pola tidak lazim	Aturan atas akses berulang dan di luar jam	Aturan dan peringatan	Uji pola simulasi
Peninjauan catatan	Telaah sampel bulanan pihak independen	Kertas kerja	Telaah kertas kerja
Pemantauan kesehatan perangkat	Deteksi kamera tidak mengirim aliran	Konfigurasi dan peringatan	Uji pemutusan kamera

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Deteksi penurunan mutu	Deteksi gambar kabur atau terhalang	Aturan deteksi	Uji penutupan lensa
Pencadangan terpisah	Salinan tidak dapat diakses dari produksi	Arsitektur cadangan	Uji akses dari produksi
Uji pemulihan berkala	Pemulihan sampel setiap semester	Laporan uji	Ulangi uji
Manajemen perubahan	Perubahan arah kamera melalui persetujuan	Catatan perubahan	Bandingkan arah aktual
Pengamanan fisik perangkat	Rumah pelindung dan deteksi manipulasi	Berita acara dan konfigurasi	Inspeksi dan uji geser
Pemusnahan media	Media dimusnahkan sebelum keluar	Berita acara	Telaah berita acara
Manajemen insiden	Prosedur mencakup skenario khas citra	Prosedur dan catatan	Telaah kelengkapan
Rantai penyimpanan bukti	Pencatatan setiap perpindahan penguasaan	Formulir rantai bukti	Telaah kelengkapan formulir

Sumber: Diolah Penulis

LAMPIRAN E TEMPLAT

PRIVACY CONTROL MAPPING

ISO/IEC 27701

Lampiran ini memuat matriks pemetaan kontrol privasi sebagaimana diuraikan pada Bab 7 dan Bab 10. Struktur kolomnya sejajar dengan Lampiran D sehingga kedua matriks dapat digabungkan menjadi satu berkas kerja.

Tabel L.E. 1: Matriks *Privacy Control Mapping Domain Tujuan dan Transparansi*

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Pendaftaran tujuan	Setiap aliran memiliki tujuan tercatat	Catatan kegiatan pemrosesan	Uji sampel terhadap penggunaan
Analisis dasar pemrosesan	Analisis penyeimbangan terdokumentasi	Dokumen analisis	Telaah mutu dan kemutakhiran
Gerbang persetujuan pemasangan	Kamera baru memerlukan persetujuan	Formulir persetujuan	Rekonsiliasi kamera dan formulir
Larangan penggunaan sekunder	Kebijakan dan mekanisme persetujuan	Kebijakan dan catatan	Telaah sampel penggunaan
Peninjauan tujuan berkala	Telaah relevansi tujuan tahunan	Kertas kerja	Telaah bukti peninjauan
Papan pemberitahuan	Tanda sebelum area, memuat identitas pengelola	Foto dan denah	Inspeksi seluruh titik masuk
Informasi lapis kedua	Kode pindai menuju keterangan lengkap	Tangkapan halaman	Uji akses melalui kode
Pemberitahuan analitik	Penyebutan adanya pengenalan otomatis	Isi papan dan halaman	Telaah kesesuaian sistem aktif

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Informasi bagi pegawai	Penjelasan tertulis saat penerimaan	Materi dan tanda terima	Telaah berkas kepegawaian

Sumber: Diolah Penulis

Tabel L.E. 2: Matriks *Privacy Control Mapping Domain* Minimalisasi dan Retensi

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Penutupan area pada perangkat	Area di luar tujuan ditutup permanen	Konfigurasi dan tampilan	Verifikasi tampilan langsung
Pembatasan jadwal perekaman	Jadwal sesuai jam operasional	Konfigurasi jadwal	Telaah rekaman di luar jadwal
Pembatasan resolusi	Resolusi sesuai kebutuhan tujuan	Konfigurasi perangkat	Telaah kesesuaian
Penonaktifan fitur tidak terpakai	Kemampuan analitik tidak dipakai dimatikan	Daftar fitur aktif	Telaah lisensi dan konfigurasi
Pembatasan kerincian keluaran	Analitik menghasilkan tingkat minimum	Konfigurasi analitik	Telaah keluaran aktual
Penghapusan metadata	Metadata dihapus sebelum publikasi	Prosedur dan hasil periksa	Periksa metadata berkas terbit
Pengaburan bawaan	Wajah diburamkan sejak penerimaan	Konfigurasi dan sampel	Telaah tampilan pemutaran
Pemulihan berotorisasi	Perlu persetujuan dua pihak dan tercatat	Catatan permintaan	Telaah sampel permintaan
Kekuatan penyamaran memadai	Teknik tidak dapat dipulihkan untuk publikasi	Standar teknis	Uji upaya pemulihan
Pemisahan tabel pemetaan	Kunci pemetaan pada sistem terpisah	Arsitektur sistem	Telaah lokasi tabel
Pembaruan pengenalan berkala	Pengenalan pelacakan diperbarui terjadwal	Konfigurasi	Telaah rentang hidup pengenalan

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Penghapusan citra pendaftaran	Citra dihapus setelah templat dibuat	Prosedur dan verifikasi	Uji keberadaan citra
Jadwal retensi per aliran	Masa simpan ditetapkan dan didokumentasikan	Jadwal retensi	Telaah kelengkapan
Penghapusan otomatis	Mekanisme terjadwal pada seluruh lapis	Konfigurasi dan catatan	Uji keberadaan rekaman lampau
Cakupan turunan dan cadangan	Metadata dan cadangan ikut terhapus	Konfigurasi	Uji sampel pada seluruh lapis
Penahanan penghapusan	Mekanisme penahanan dan pencabutan	Daftar penahanan	Telaah daftar dan tanggal

Sumber: Diolah Penulis

Tabel L.E. 3: Matriks *Privacy Control Mapping Domain* Hak Subjek dan Pemroses

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Kanal penerimaan permintaan	Kanal jelas dan mudah diakses	Informasi kontak	Uji pengajuan
Register permintaan	Seluruh permintaan tercatat	Berkas register	Telaah kelengkapan
Verifikasi identitas proporsional	Verifikasi tanpa pengumpulan berlebihan	Prosedur	Telaah sampel penanganan
Kemampuan pencarian	Pencarian berdasarkan waktu dan lokasi	Konfigurasi sistem	Uji simulasi pencarian
Pengaburan selektif	Individu lain diburamkan pada hasil	Sampel hasil	Uji simulasi permintaan
Pemantauan tenggat	Peringatan sebelum batas waktu	Konfigurasi	Telaah ketepatan waktu

Kontrol	Rancangan Penerapan	Bukti	Metode Uji
Dokumentasi penolakan	Alasan tercatat dan disampaikan	Sampel surat	Telaah sampel penolakan
Penilaian vendor	Kuesioner dan telaah kemampuan	Laporan penilaian	Telaah dokumen
Perjanjian pemrosesan	Klausul lengkap sesuai kerangka	Perjanjian	Telaah kelengkapan klausul
Daftar subpemroses	Daftar terkini dan mekanisme persetujuan	Daftar	Telaah kemutakhiran
Larangan penggunaan sendiri	Klausul larangan pelatihan model	Perjanjian	Telaah keberadaan klausul
Pemusnahan akhir kontrak	Kewajiban dan bukti pemusnahan	Sertifikat	Telaah kontrak berakhir
Register pengungkapan	Pencatatan setiap penyerahan	Berkas register	Rekonsiliasi catatan sistem
Pembatasan wilayah	Wilayah dibatasi melalui konfigurasi	Konfigurasi	Verifikasi lokasi aktual
Penilaian dampak	Kajian sebelum sistem baru	Laporan penilaian	Telaah pelaksanaan
Prosedur insiden privasi	Prosedur dan jalur notifikasi	Prosedur dan catatan	Uji simulasi tenggat

Sumber: Diolah Penulis

LAMPIRAN F TEMPLAT AUDIT *CHECKLIST DAN EVIDENCE REGISTER*

Lampiran ini memuat instrumen audit yang menggabungkan daftar periksa pemeriksaan dengan register bukti. Instrumen digunakan oleh audit internal maupun sebagai persiapan menghadapi audit eksternal dan pemeriksaan otoritas.

Tabel L.F. 1: Struktur Kolom Audit Checklist

Kolom	Panduan Pengisian
Nomor butir	Pengenal urutan butir pemeriksaan
Domain	Kelompok kontrol yang diperiksa
Kriteria audit	Pernyataan keadaan yang seharusnya
Metode pengujian	Telaah dokumen, wawancara, observasi, uji teknis
Ukuran sampel	Jumlah dan cara pemilihan sampel
Bukti yang diminta	Artefak yang harus disediakan auditee
Hasil pengujian	Sesuai, sesuai sebagian, tidak sesuai
Uraian temuan	Penjelasan ketidaksesuaian bila ada
Tingkat temuan	Mayor, minor, atau peluang perbaikan
Rekomendasi	Saran perbaikan
Pemilik tindakan	Jabatan penanggung jawab
Tenggat perbaikan	Batas waktu penyelesaian
Status tindak lanjut	Terbuka, berjalan, selesai, diverifikasi

Sumber: Diolah Penulis

Tabel L.F. 2: Butir Audit Domain Tata Kelola dan Aset

No	Kriteria Audit	Metode
1	Kebijakan pengawasan visual tersedia, disahkan, dan mutakhir	Telaah dokumen
2	Seluruh kamera terpasang tercatat dalam inventaris	Rekonsiliasi lapangan

No	Kriteria Audit	Metode
3	Setiap aliran memiliki pemilik aset yang ditetapkan	Telaah inventaris
4	Setiap aliran memiliki tujuan dan dasar pemrosesan tercatat	Telaah catatan pemrosesan
5	Pemasangan kamera dalam periode audit melalui persetujuan	Uji sampel
6	Klasifikasi ditetapkan dan sesuai sensitivitas aktual	Uji sampel
7	Pemetaan aliran data tersedia dan mutakhir	Telaah dokumen
8	Forum tata kelola bersidang dan keputusannya tercatat	Telaah notulen
9	Pelatihan etika pengawasan dilaksanakan bagi operator	Telaah daftar hadir
10	Tinjauan manajemen dilaksanakan dan mencakup indikator privasi	Telaah laporan

Sumber: Diolah Penulis

Tabel L.F. 3: Butir Audit Domain Kontrol Teknis

No	Kriteria Audit	Metode
11	Tidak terdapat akun bersama pada sistem manajemen video	Uji teknis
12	Hak akses sesuai peran dan ditinjau dalam periode audit	Uji sampel
13	Akun personel yang berhenti telah dicabut tepat waktu	Rekonsiliasi daftar
14	Autentikasi berfaktor ganda aktif pada fungsi sensitif	Uji teknis
15	Kredensial bawaan pabrik telah diubah pada seluruh perangkat	Uji sampel
16	Jaringan kamera tersegmentasi dan akses keluar dibatasi	Uji teknis
17	Aliran dan penyimpanan terenkripsi sesuai kebijakan	Uji teknis
18	Kunci enkripsi dikelola terpisah dari data	Telaah arsitektur
19	Peristiwa wajib tercatat termasuk alasan akses	Uji teknis dan sampel
20	Catatan akses ditinjau berkala oleh pihak independen	Telaah kertas kerja

No	Kriteria Audit	Metode
21	Pemantauan kesehatan perekaman berjalan dan peringatan ditindaklanjuti	Telaah catatan
22	Uji pemulihan dilaksanakan dan berhasil	Telaah laporan
23	Perubahan konfigurasi kamera melalui persetujuan	Uji sampel
24	Media penyimpanan yang keluar dimusnahkan dengan bukti	Telaah berita acara

Sumber: Diolah Penulis

Tabel L.F. 4: Butir Audit Domain Privasi

No	Kriteria Audit	Metode
25	Papan pemberitahuan terpasang pada seluruh titik masuk	Observasi menyeluruh
26	Isi pemberitahuan mencerminkan kemampuan sistem yang aktif	Telaah dan uji teknis
27	Tidak terdapat kamera pada area dengan ekspektasi privasi tinggi	Observasi menyeluruh
28	Cakupan pandang dibatasi melalui penutupan area	Observasi tampilan
29	Jadwal retensi ditetapkan dan dijalankan otomatis	Uji teknis
30	Rekaman melampaui masa simpan tidak ditemukan di seluruh lapis	Uji sampel
31	Penahanan penghapusan ditinjau dan dicabut bila selesai	Telaah daftar
32	Permintaan subjek data ditangani tepat waktu dan tercatat	Telaah register
33	Kemampuan pengaburan selektif tersedia dan berfungsi	Uji simulasi
34	Perjanjian pemrosesan tersedia untuk seluruh pemroses aktif	Telaah kontrak
35	Register pengungkapan dipelihara dan lengkap	Rekonsiliasi
36	Wilayah penyimpanan sesuai kebijakan dan diverifikasi	Uji teknis
37	Penilaian dampak dilaksanakan sebelum sistem baru diterapkan	Telaah dokumen
38	Fitur analitik tidak terpakai telah dinonaktifkan	Uji teknis

No	Kriteria Audit	Metode
39	Pengujian akurasi model dilaksanakan termasuk per kelompok	Telaah laporan
40	Insiden privasi tercatat dan ditindaklanjuti sesuai prosedur	Telaah register

Sumber: Diolah Penulis

Tabel L.F. 5: Struktur Evidence Register

Kolom	Panduan Pengisian
Nomor bukti	Pengenal urutan artefak
Kontrol terkait	Rujukan kode kontrol
Nama bukti	Sebutan artefak
Jenis bukti	Dokumen, konfigurasi, catatan sistem, kertas kerja
Periode yang dicakup	Rentang waktu keberlakuan bukti
Lokasi penyimpanan	Sistem dan jalur penyimpanan
Penanggung jawab	Jabatan penghimpun bukti
Frekuensi penghimpunan	Bulanan, triwulanan, tahunan, per kejadian
Tanggal terakhir dihimpun	Waktu pemutakhiran terakhir
Status kelengkapan	Lengkap, sebagian, belum tersedia

Sumber: Diolah Penulis

DAFTAR PUSTAKA

- Badan Siber dan Sandi Negara. (2023). Pedoman penerapan manajemen keamanan informasi bagi penyelenggara sistem elektronik. Jakarta: Badan Siber dan Sandi Negara.
- Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Toronto: Information and Privacy Commissioner of Ontario.
- European Union Agency for Cybersecurity. (2021). Data protection engineering: From theory to practice. Athens: ENISA.
- European Union Agency for Cybersecurity. (2022). Remote identity proofing: Attacks and countermeasures. Athens: ENISA.
- Gonzalez, R. C., & Woods, R. E. (2018). *Digital image processing* (4th ed.). New York: Pearson.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. Cambridge: MIT Press.
- International Organization for Standardization. (2015). ISO/IEC 27017:2015 Code of practice for information security controls based on ISO/IEC 27002 for *cloud* services. Geneva: ISO.
- International Organization for Standardization. (2018). ISO 31000:2018 Risk management — Guidelines. Geneva: ISO.
- International Organization for Standardization. (2018). ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques. Geneva: ISO.
- International Organization for Standardization. (2019). ISO/IEC 27018:2019 Code of practice for protection of personally identifiable information in public *clouds* acting as PII processors. Geneva: ISO.
- International Organization for Standardization. (2019). ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Geneva: ISO.

- International Organization for Standardization. (2020). ISO/IEC 29134:2023 Guidelines for privacy impact assessment. Geneva: ISO.
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO.
- International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO.
- International Organization for Standardization. (2022). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: ISO.
- International Organization for Standardization. (2023). ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system. Geneva: ISO.
- Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to biometrics. New York: Springer.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Jakarta: Sekretariat Negara.
- National Institute of Standards and Technology. (2012). NIST Special Publication 800-30 *Revision 1*: Guide for conducting risk assessments. Gaithersburg: NIST.
- National Institute of Standards and Technology. (2018). NIST Special Publication 800-37 *Revision 2*: Risk management framework for information systems and organizations. Gaithersburg: NIST.
- National Institute of Standards and Technology. (2020). NIST Privacy Framework Version 1.0: A tool for improving privacy through enterprise risk management. Gaithersburg: NIST.
- National Institute of Standards and Technology. (2023). NIST AI Risk Management Framework 1.0. Gaithersburg: NIST.

- Pemerintah Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah. Jakarta: Sekretariat Negara.
- Pemerintah Republik Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Jakarta: Sekretariat Negara.
- Solove, D. J. (2008). *Understanding privacy*. Cambridge: Harvard University Press.
- Szeliski, R. (2022). *Computer vision: Algorithms and applications* (2nd ed.). Cham: Springer.
- World Economic Forum. (2022). *Responsible use of technology: The IEEE approach*. Geneva: World Economic Forum.
- Wright, D., & De Hert, P. (Eds.). (2012). *Privacy impact assessment*. Dordrecht: Springer.

DAFTAR SINGKATAN

Singkatan	Kepanjangan
AI	<i>Artificial Intelligence</i> , kecerdasan buatan
API	Application Programming Interface, antarmuka pemrograman aplikasi
CCTV	Closed Circuit Television, televisi sirkuit tertutup
CIA	Confidentiality, Integrity, Availability
DPIA	Data Protection Impact Assessment, penilaian dampak perlindungan data
DPO	Data Protection Officer, petugas perlindungan data
EXIF	Exchangeable <i>Image</i> File Format
FPS	Frames Per Second, bingkai per detik
GPU	Graphics Processing Unit
HSM	Hardware Security Module, modul keamanan perangkat keras
IAM	Identity and Access Management
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
KPI	Key Performance Indicator, indikator kinerja utama
KRI	Key Risk Indicator, indikator risiko utama
MFA	Multi-Factor Authentication, autentikasi berfaktor ganda
NIST	National Institute of Standards and Technology
NVR	Network Video Recorder, perekam video jaringan
PACS	Picture Archiving and Communication System
PIA	Privacy Impact Assessment, penilaian dampak privasi

Singkatan	Kepanjangan
PII	Personally Identifiable Information, informasi pribadi
PIMS	Privacy Information Management System
RBAC	Role Based Access Control, kontrol akses berbasis peran
RTSP	<i>Real time Streaming</i> Protocol
SIEM	Security Information and Event Management
SLA	Service Level Agreement, perjanjian tingkat layanan
SOA	Statement of Applicability, pernyataan keberlakuan
UU PDP	Undang-Undang Pelindungan Data Pribadi
VMS	Video Management System, sistem manajemen video
VPN	Virtual Private Network
WORM	Write Once Read Many

GLOSARIUM

A

Akuisisi : Tahap pengambilan citra oleh perangkat sensor hingga menghasilkan berkas digital.

Analitik video : Penerapan algoritma pemrosesan citra terhadap aliran video secara berkelanjutan untuk menghasilkan peringatan atau ringkasan otomatis.

Anonimisasi : Proses menghilangkan kemampuan mengaitkan data dengan individu secara permanen sehingga data tidak lagi berkedudukan sebagai data pribadi.

Aset informasi : Segala sesuatu yang bernilai bagi organisasi dan berkaitan dengan informasi, mencakup data, media, perangkat, perangkat lunak, dan layanan.

B

Bukti digital : Informasi elektronik yang dapat digunakan untuk membuktikan suatu peristiwa dan nilainya bergantung pada keaslian serta keutuhannya.

C

Citra adversarial : Citra yang dimodifikasi dengan perubahan kecil tak kasatmata sehingga menyebabkan model pembelajaran mesin menghasilkan keluaran keliru.

Citra digital : Representasi numerik dari intensitas cahaya yang tersusun sebagai matriks piksel.

D

Deepfake : Media sintetis yang dihasilkan atau dimodifikasi model generatif sehingga menampilkan peristiwa yang tidak pernah terjadi.

Deteksi keaslian : Mekanisme yang memastikan bahwa masukan biometrik berasal dari individu hidup, bukan dari foto, tayangan layar, atau topeng.

Deteksi objek : Proses menemukan keberadaan dan posisi objek tertentu dalam citra, dinyatakan sebagai kotak pembatas beserta label kelas.

E

Ekstraksi fitur : Penghitungan besaran numerik yang merepresentasikan karakteristik objek pada citra.

Enkripsi saat diam : Perlindungan kriptografis terhadap data yang tersimpan pada media penyimpanan.

Enkripsi saat transit : Perlindungan kriptografis terhadap data yang sedang berpindah antartitik.

I

Identifikasi : Mode operasi biometrik berupa pencocokan satu banding banyak untuk menemukan identitas seseorang dari basis data.

Inferensi : Proses menggunakan model terlatih untuk menghasilkan keluaran atas masukan baru.

Informasi pribadi : Setiap informasi mengenai orang perseorangan yang teridentifikasi atau dapat diidentifikasi.

K

Kematangan : Tingkat kebakuan, konsistensi, dan keterukuran proses pengendalian pada suatu organisasi.

Keteridentifikasian : Tingkat kemungkinan seseorang dikenali dari suatu data, berada pada spektrum antara teridentifikasi penuh dan anonim.

Kustodian : Pihak yang mengoperasikan dan memelihara aset sesuai keputusan pemilik aset.

M

Metadata : Informasi yang menyertai berkas citra dan tidak tampak pada gambarnya, mencakup perangkat, waktu, lokasi, dan riwayat penyuntingan.

Minimalisasi data : Prinsip bahwa data yang diproses harus memadai, relevan, dan terbatas pada yang diperlukan bagi tujuan.

N

Nirsangkal : Sifat yang menyebabkan pihak yang melakukan suatu tindakan tidak dapat mengingkarinya di kemudian hari.

P

Pemilik aset : Pihak yang bertanggung jawab atas keputusan mengenai aset, termasuk klasifikasi, otorisasi akses, dan penetapan masa simpan.

Pemroses informasi pribadi : Pihak yang memproses informasi pribadi atas nama dan berdasarkan instruksi pengendali.

Penahanan penghapusan : Mekanisme mengecualikan data tertentu dari jadwal pemusnahan karena diperlukan bagi proses hukum atau investigasi.

Pengaburan berotorisasi : Pola pengendalian berupa pengaburan otomatis yang hanya dapat dipulihkan melalui permintaan yang disetujui dan tercatat.

Pengenali ulang : Kemampuan mengenali bahwa objek yang muncul pada kamera berbeda merupakan objek yang sama.

Pengendali informasi pribadi : Pihak yang menentukan tujuan dan cara pemrosesan informasi pribadi.

Peracunan data : Penyisipan data yang dirancang khusus ke dalam himpunan pelatihan sehingga model memiliki perilaku menyimpang.

Prapemrosesan : Tahap penyiapan citra agar dapat dianalisis dengan hasil yang lebih andal.

Pseudonimisasi : Penggantian pengenalan langsung dengan pengenalan buatan, dengan kemampuan pengaitan kembali yang disimpan terpisah.

R

Rantai penyimpanan bukti : Pencatatan berkelanjutan atas setiap perpindahan penguasaan bukti sejak diidentifikasi hingga digunakan.

Retensi : Periode penyimpanan data yang ditetapkan berdasarkan tujuan pemrosesan dan kewajiban yang berlaku.

S

Segmentasi citra : Pemisahan citra menjadi wilayah-wilayah yang bermakna, misalnya memisahkan objek dari latar belakang.

Silsilah data : Catatan asal usul data dan model yang menelusuri sumber, versi, dan dasar pemrosesan.

Steganografi : Teknik menyisipkan data tersembunyi ke dalam nilai piksel citra sehingga tidak terdeteksi secara visual.

Subjek data : Individu yang menjadi subjek dari suatu informasi pribadi.

T

Tanda air dinamis : Penanda yang memuat identitas pengguna dan waktu, ditampilkan di atas gambar untuk memungkinkan penelusuran penyebaran.

Templat biometrik : Representasi numerik dari ciri biometrik yang digunakan untuk pencocokan identitas.

Titik kendali : Tahap pada siklus hidup tempat suatu kontrol ditempatkan agar paling efektif.

V

Vektor fitur : Representasi berdimensi tinggi hasil pemrosesan model yang merepresentasikan karakteristik objek atau wajah.

Verifikasi : Mode operasi biometrik berupa pencocokan satu banding satu untuk memastikan seseorang adalah orang yang diklaimnya.

INDEKS

A

Akuisisi — 1, 5, 18, 29, 38, 41, 88, 209
Analitik video — 2, 13, 25, 26, 203, 246, 250
Anonimisasi — 66, 106, 124, 163, 173, 203, 224, 246
Arsitektur — 27, 30, 78, 138, 143, 147, 181, 234
Aset informasi — 10, 13, 32, 98, 246, 250
Audit — 11, 41, 94, 105, 148, 170, 194, 237
Autentikasi — 25, 90, 96, 120, 135, 207, 230, 244

B

Bias — 7, 55, 67, 88, 128, 140, 151, 184
Biometrik — 3, 22, 65, 77, 137, 159, 173, 246
Bukti digital — 3, 4, 150, 181, 246, 250

C

Cadangan — 4, 42, 76, 104, 130, 152, 207, 224
Citra adversarial — 23, 55, 246, 250
Cloud — 2, 29, 53, 146, 204, 241, 242, 250

D

Daftar risiko — 60, 63, 78, 132, 180, 207, 213, 222
Deepfake — 51, 246, 250
Deteksi keaslian — 25, 51, 199, 246, 250

E

Enkripsi — 5, 35, 69, 121, 137, 163, 199, 215
EXIF — 28, 244, 250
Ekstraksi fitur — 21, 22, 247, 250

G

Gerbang persetujuan — 156, 173, 177, 178, 189, 206, 233, 250
Glosarium — 246, 250

H

Hak subjek data — 8, 100, 102, 107, 113, 170, 182, 227

I

Identifikasi — 6, 22, 64, 77, 114, 154, 179, 226
Inferensi — 27, 57, 115, 124, 125, 130, 183, 247
Informasi pribadi — 10, 98, 102, 106, 154, 165, 244, 248
Insiden — 1, 50, 85, 128, 150, 179, 189, 208
Inventaris — 3, 44, 96, 149, 189, 206, 213, 221

K

Kematangan — 2, 8, 57, 174, 190, 191, 208, 247
Kerahasiaan — 3, 8, 33, 35, 58, 86, 103, 185
Keteridentifikasian — 17, 20, 65, 66, 67, 247, 251

Ketersediaan — 2, 4, 35, 84, 100, 142, 147, 192

Keutuhan — 3, 16, 36, 49, 89, 120, 137, 200

Klasifikasi — 4, 21, 34, 85, 120, 147, 209, 238

Kriptografi — 11, 37, 83, 90, 137, 138, 181, 247

Kustodian — 11, 38, 39, 40, 99, 177, 220, 247

L

Lampiran — 63, 97, 153, 192, 220, 222, 229, 237

M

Matriks kontrol — 14, 95, 97, 173, 188, 191, 213, 222

Metadata — 4, 26, 34, 79, 129, 160, 201, 221

Minimalisasi — 3, 8, 20, 72, 113, 120, 161, 234

Model — 2, 20, 51, 103, 145, 174, 200, 224

N

Nirsangkal — 4, 37, 248, 251

P

Papan pemberitahuan — 196, 197, 203, 207, 213, 217, 224, 239

Pelatihan — 2, 55, 87, 111, 150, 171, 193, 214

Pemantauan — 22, 60, 86, 104, 140, 168, 185, 210

Pembatasan tujuan — 3, 4, 7, 8, 71, 75, 251

Pemilik aset — 38, 40, 127, 177, 209, 217, 230, 247

Pemroses — 2, 27, 65, 88, 115, 148, 179, 218

Pemusnahan — 41, 89, 104, 129, 148, 170, 206, 231

Penahanan penghapusan — 34, 96, 112, 153, 167, 212, 223, 239

Pengaburan — 4, 71, 112, 127, 163, 174, 201, 234

Pengendali — 2, 13, 38, 76, 106, 141, 175, 192

Pengenalan wajah — 1, 19, 24, 56, 68, 78, 157, 161

Peracunan data — 55, 248, 252

Peran — 1, 29, 51, 88, 118, 143, 186, 215

Pikselasi — 20, 66, 162, 163, 252

Prapemrosesan — 19, 20, 248, 252

Privasi sejak perancangan — 31, 78, 79, 252

Pseudonimisasi — 66, 164, 165, 182, 248, 252

R

Rantai penyimpanan bukti — 37, 38, 151, 232, 248, 252

Retensi — 2, 38, 110, 125, 165, 176, 193, 220

Risiko — 3, 26, 55, 75, 111, 139, 180, 208

S

Segmentasi — 5, 22, 92, 119, 139, 211, 223, 238

Segmentasi jaringan — 90, 92, 96, 118, 139, 215, 217, 231

Silsilah data — 125, 183, 214, 249, 252

Siklus hidup — 11, 18, 114, 128, 154, 175, 191, 222

Steganografi — 29, 249, 252

Studi kasus — 14, 195, 196, 197, 200, 201, 203, 204

Subjek data — 7, 60, 100, 108, 150, 170, 208, 226

T

Tanda air — 87, 118, 126, 130, 182, 183, 223, 249

Templat biometrik — 7, 33, 121, 137, 154, 164, 171, 249

Titik kendali — 13, 17, 116, 130, 249, 252

Transparansi — 3, 59, 70, 72, 117, 157, 158, 233

V

Vektor fitur — 21, 154, 221, 249, 252

Verifikasi — 2, 36, 80, 124, 146, 163, 198, 230

Video *analytics* — 1, 25, 203, 252

BIOGRAFI PENULIS



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

Nungky Awang Chandra, lahir di Semarang 1973. Penulis selain dosen teknik informatika fasilkom universitas mercubuana, juga berprofesi sebagai auditor sistem manajemen keamanan informasi ISO 27001, ISO22301, ISO 27701, ISO 20000, ISO 42001 yang *tereregister* di BSSN. Penulis merupakan lulusan pendidikan Sarjana S1 jurusan Fisika Komputasi Institut Teknologi Bandung pada tahun 1998. Kemudian pada tahun 2007 melanjutkan pendidikan master dibidang Magister Teknologi Infomasi Universitas Indonesia, menyelesaikan studinya pada tahun 2009. Pada tahun 2022 penulis juga 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 juga menyelesaikan studi postgraduted cyber security di Massachusetts Institute of Technology (MIT).

Penulis memiliki kepakaran dibidang keamanan siber, pengembangann aplikasi, drone. Dan untuk mewujudkan karier sebagai dosen profesional, penulis pun aktif sebagai peneliti dibidang kepakarannya tersebut. Beberapa penelitian yang telah dilakukan didanai oleh internal perguruan tinggi dan juga Kemenristek DIKTI. Selain peneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini. Adapun untuk koresponden dengan penulis dapat email ke penulis dengan email : nungkyac707@gmail.com



Dr. Hadi Santoso, S.Kom., M.Kom.

Penulis. adalah akademisi, peneliti, dan praktisi di bidang Ilmu Komputer yang memiliki perhatian khusus pada *Artificial Intelligence, Machine Learning, Deep learning, Computer Vision, Image processing, Data Mining*, dan *Data Science*. Ia menyelesaikan pendidikan Sarjana dan Magister di bidang Ilmu Komputer di Universitas Budi Luhur, kemudian meraih gelar Doktor (S3) Ilmu Komputer dari Universitas Gadjah Mada. Ia juga menyelesaikan pendidikan profesi Insinyur di Universitas Mercu Buana. Penelitian doktoralnya berfokus pada *real-time multiple face recognition* dengan mengintegrasikan modifikasi AdaBoost Viola-Jones, 2D DWT-PCA, dan struktur indeks K-D Tree.

Dalam kegiatan akademik, Hadi Santoso aktif mengajar berbagai mata kuliah, antara lain *Image processing, Deep learning, Computer Vision, Algorithms and Programming, Introduction to Data Mining, Advanced Data Mining, Mathematical Tools for Data Science, Digital Forensics*, serta *Research Methodology for Information Technology*. Pengalaman tersebut memperkuat minat akademiknya pada pengembangan metode komputasi cerdas dan penerapan kecerdasan buatan untuk menyelesaikan berbagai permasalahan nyata.

Selain mengajar, ia aktif melaksanakan penelitian dalam bidang *computer vision, artificial intelligence, machine learning, image classification, object recognition, geospatial analysis*, dan *intelligent systems*. Beberapa penelitiannya membahas pengenalan dan klasifikasi citra berbasis *deep learning*, prediksi berbasis *Random Forest*, serta pengembangan sistem navigasi berbasis visi untuk membantu penyandang tunanetra melalui *multimodal scene understanding*.

Karya ilmiahnya telah dipublikasikan pada berbagai jurnal nasional dan internasional dengan topik yang mencakup *transfer learning, klasifikasi citra, EfficientNet, ResNet, machine learning*, analisis spasio-temporal, dan kecerdasan buatan. Salah satu publikasinya, *A Hybrid Model for Dry Waste Classification using Transfer Learning and Dimensionality Reduction*, diterbitkan pada *International Journal on*

Informatics Visualization (JOIV) yang tercantum sebagai jurnal Scopus Q3 dalam CV. Ia juga aktif mempresentasikan hasil penelitian dalam forum ilmiah internasional, termasuk konferensi di Guangzhou, China, dan Kota Kinabalu, Malaysia.

Dalam bidang penulisan buku, ia telah menghasilkan sejumlah karya, antara lain *Konsep Kriptografi dan Steganografi dalam Mewujudkan Keamanan Digital di Era Industri 5.0*, *Pembelajaran Mesin dan Kecerdasan Buatan: Teori dan Aplikasi Praktis*, *Pemrograman Smart Web: Panduan Lengkap Membuat Aplikasi Cerdas dengan Semantic Web dan PHP*, serta *Algoritma dan Pemrograman dengan Bahasa Python*.

Kontribusinya juga diwujudkan melalui berbagai Hak Kekayaan Intelektual (HKI) berupa program komputer, mulai dari aplikasi *image* retrieval berbasis wajah, pemetaan industri berbasis Web-GIS, analisis data berbasis clustering, sistem surat digital, hingga aplikasi tanda tangan dan validasi berbasis QR Code.

Pada tingkat internasional, pada tahun 2026 ia tercatat memiliki pengalaman sebagai Guest Lecturer/Visiting Professor di Faculty of Information Technology and Big Data Analysis, Financial University, Moscow, Russia.

Melalui kegiatan pendidikan, penelitian, publikasi, pengabdian kepada masyarakat, penulisan buku, dan pengembangan kekayaan intelektual, Dr. Ir. Hadi Santoso, S.Kom., M.Kom. terus berkontribusi dalam pengembangan ilmu komputer dan pemanfaatan kecerdasan buatan, khususnya untuk menghasilkan teknologi yang inovatif, aplikatif, dan memberikan manfaat bagi masyarakat.

Bidang keahlian: *Artificial Intelligence, Machine Learning, Deep learning, Computer Vision, Image processing, Data Mining, dan Data Science*.



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, pendidikan S2 di Preston University Islamabad Pakistan dan saat ini sedang menyelesaikan S3 di Universiti Malaysia Kelantan pada bidang *Data Science*. Penulis adalah Dosen Tetap Universitas Mercu Buana Jakarta. Buku populer yang telah dihasilkan adalah Pemrograman Mobile dengan Flutter, Pemrograman Java, Aplikasi Mobile Teori dan Praktek, Teknik 2D/3D Blender Untuk Pemula hingga Ahli, Bahasa Pemrograman Python dan Pembelajaran Mesin dan Kecerdasan Buatan Teori dan Aplikasi Praktis. Selain itu juga telah menulis buku tentang Tata Kelola Teknologi Informasi. Untuk menghubungi penulis di email: mhd.yusuf@mercubuana.ac.id.



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

Ketertarikan penulis terhadap ilmu komputer dimulai pada tahun 2010 silam. Hal tersebut membuat penulis memilih untuk masuk ke Sekolah Perguruan Tinggi Di bidang Sistem Informasi. Setelah lulus S1, 2 tahun kemudian, penulis menyelesaikan studi S2 di prodi Teknik Informatika Program Pasca Sarjana Universitas Raharja. Penulis memiliki kepakaran dibidang *Web Technology dan Data Science*. Dan untuk mewujudkan karir sebagai dosen profesional, penulis pun aktif sebagai peneliti dibidang kepakarannya tersebut. Beberapa penelitian yang telah dilakukan didanai oleh internal perguruan tinggi dan juga Kemenristek DIKTI.

Selain peneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini. Dengan tujuan mengembangkan solusi perangkat lunak inovatif yang memecahkan tantangan bisnis dengan menggunakan keterampilan pemrograman dan pengetahuan teknologi terkini. Terus meningkatkan kemampuan teknis dan kepemimpinan melalui pengalaman praktis dan pembelajaran berkelanjutan. Email Penulis: mays41946@gmail.com.



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

Diva Alifta Chandra lahir di Purwokerto pada tahun 2001. Ia merupakan seorang auditor sistem manajemen keamanan informasi yang tersertifikasi ISO 27001 dan ISO 27701 dari lembaga internasional IRCA (United Kingdom) dan PECB (Canada). Penulis menyelesaikan pendidikan sarjana (S1) di bidang Biomedical Engineering dari University of Technology Malaysia (UTM), kemudian melanjutkan studi pascasarjana

dan meraih gelar Master of Data Science dari University of Malaya (UM) dengan disertasi yang berfokus pada *Algorithmic Social Computing*. Selain berkarier sebagai auditor, penulis juga 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. Penulis secara aktif meneliti serta menulis artikel ilmiah seputar *social computing*, dengan harapan dapat memberikan kontribusi nyata bagi kemajuan bangsa dan negara. Untuk korespondensi, penulis dapat dihubungi melalui email: divaac56@gmail.com

KERANGKA KERJA PENGENDALIAN KEAMANAN INFORMASI DAN PERLINDUNGAN DATA PRIBADI PADA IMAGE PROCESSING

Berbasis ISO/IEC 27002 dan ISO/IEC 27701

Kamera kini ada di mana-mana. Kamera pengawas di lobi dan koridor, kamera ponsel di tangan setiap pegawai, sensor visual di lini produksi, perangkat pencitraan di fasilitas kesehatan, hingga kamera pada kendaraan dan wahana udara nirawak. Yang berubah bukan hanya jumlahnya, melainkan perannya. Citra tidak lagi sekadar arsip pasif yang ditinjau ketika terjadi insiden, melainkan masukan bagi keputusan otomatis yang berdampak langsung terhadap individu. Perubahan itu berlangsung jauh lebih cepat daripada kematangan pengendaliannya. Banyak organisasi telah mengoperasikan sistem pemrosesan citra selama bertahun-tahun tanpa pernah melakukan inventarisasi aset citra, penilaian risiko privasi, maupun penetapan periode retensi yang eksplisit. Kesenjangan ini bukan disebabkan oleh ketiadaan niat baik, melainkan oleh ketiadaan panduan yang menghubungkan standar pengendalian dengan karakteristik teknis pemrosesan citra. Buku ini hadir untuk mengisi kesenjangan tersebut. Dengan menggabungkan ISO/IEC 27002 sebagai rujukan kontrol keamanan informasi dan ISO/IEC 27701 sebagai rujukan pengelolaan informasi privasi, buku ini menyusun satu kerangka kerja terpadu yang dapat digunakan organisasi untuk mengidentifikasi risiko, memilih kontrol, menerapkan pengamanan, dan mengevaluasi efektivitasnya sepanjang siklus hidup pemrosesan citra — mulai dari pengumpulan, transmisi, penyimpanan, pengolahan, pelatihan model kecerdasan buatan, penyajian, pembagian, hingga pemusnahan. QWEWQ Yang membedakan buku ini adalah sifatnya yang aplikatif. Pembahasan tidak berhenti pada penjelasan standar, melainkan menerjemahkan maksud setiap kontrol menjadi rancangan penerapan yang konkret, disertai bukti implementasi yang dihasilkan dan cara mengujinya. Lebih dari seratus tabel kerja di dalamnya disusun agar dapat langsung disalin dan disesuaikan oleh pembaca sebagai instrumen kerja, bukan sekadar sebagai ilustrasi. Pengendalian keamanan informasi dan perlindungan data pribadi pada pemrosesan citra bukan merupakan proyek yang selesai, melainkan kemampuan yang dibangun dan dipelihara. Teknologi akan terus berkembang dan bersamaan dengan itu akan muncul risiko yang belum terbayangkan saat ini. Organisasi yang memiliki kerangka kerja yang berjalan, inventaris yang terpelihara, penilaian yang dimutakhirkan, dan budaya yang menempatkan kepentingan individu sebagai pertimbangan akan mampu menyesuaikan diri terhadap perkembangan tersebut.

Keunggulan Buku:

- Memadukan dua standar sekaligus. Keamanan informasi dan perlindungan data pribadi dikelola sebagai satu program terpadu, bukan dua program terpisah yang menghasilkan duplikasi dan celah.
- Berangkat dari pemahaman teknis. Tiga bab pertama membangun fondasi mengenai anatomi pemrosesan citra, sehingga diskusi pengendalian dapat dilakukan pada kedalaman yang memadai.
- Menyediakan instrumen siap pakai. Enam lampiran memuat templat asset register, risk register, penilaian dampak privasi, pemetaan kontrol keamanan dan privasi, serta daftar periksa audit dan register bukti.
- Setiap kontrol disertai buktinya. Rancangan kontrol selalu menyebutkan artefak yang dihasilkan dan metode pengujiannya, karena kontrol yang tidak dapat diuji tidak dapat diandalkan.
- Dilengkapi enam studi kasus nyata. Mulai dari CCTV perkantoran, pengenalan wajah di pabrik, inspeksi mutu produksi, citra medis, analitik video berbasis kecerdasan buatan, hingga pemrosesan berbasis awan.
- Menutup dengan peta jalan yang konkret. Rencana implementasi 30–60–90 hari beserta penanggung jawab dan keluaran setiap kegiatan.

"INOVASI BERBASIS CITRA AKAN LEBIH BERMAKNA APABILA PRIVASI DAN KEAMANAN MENJADI BAGIAN DARI RANCANGANNYA SEJAK AWAL."