

Audit Data Privacy: untuk UU PDP Compliance

Onno W. Purbo
onno@indo.net.id
onno@itts.ac.id
Twitter onnowpurbo

**Institut Teknologi Tangerang Selatan (ITTS)
OnnoCenter
2025**

Lisensi

Karya ini dilisensikan di bawah lisensi **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)**.

Artinya, **siapa pun bebas untuk menggunakan, menyalin, membagikan, dan mengadaptasi** materi ini, **dengan syarat**:

- **Memberikan atribusi yang sesuai** (menyebut sumber asli),
- **Menyertakan lisensi yang sama** jika dimodifikasi atau dikembangkan lebih lanjut.

Lihat detail lisensi di sini <https://creativecommons.org/licenses/by-nd/4.0/legalcode.id>

Disclaimer

Dokumen ini disediakan *as-is* untuk tujuan edukasi dan operasional TI, **bukan *legal advice***; seluruh rekomendasi, *playbook*, dan pemetaan Pasal UU PDP → kontrol teknis adalah *best-effort* berbasis praktik industri dan sumber yang dirujuk di naskah (termasuk statistik kebocoran data Indonesia ≈94,22 juta akun, kewajiban notifikasi ≤**3×24 jam**, serta sanksi administratif hingga **2% pendapatan**), namun **tanggung jawab penerapan, akurasi data, dan kepatuhan akhir berada pada organisasi pengguna**. Nama produk/alat (termasuk **Cyber Rank**) digunakan sebagai ilustrasi arsitektur dan *evidence pack*—**bukan endorsement**—dan **tidak menggantikan** kewajiban uji tuntas, penilaian risiko, maupun konsultasi hukum setempat. Contoh dataset/regex/masking adalah contoh umum; **jangan** memproses data pribadi nyata tanpa dasar hukum yang sah, *DPIA*, dan pengendalian keamanan yang memadai. Regulasi dapat berubah; **verifikasi periodik** terhadap kebijakan regulator dan kontrak vendor tetap wajib.

Executive Summary

Buku *Audit Data Privacy untuk Compliance UU PDP* hadir pada momentum kritis ketika **Indonesia mencatat lebih dari 94 juta akun terdampak kebocoran data hanya dalam kurun 2020–2023** (sumber: Kominfo, BSSN), menandakan betapa masifnya risiko privasi yang dihadapi sektor publik maupun swasta. Novelty utama buku ini adalah penyajian panduan **praktis dan teknis** bagi profesional IT, dengan kerangka pemetaan Pasal UU PDP → kontrol teknologi, didukung *automated tools* dan *evidence pack* siap audit. Lebih jauh, dokumen ini mengintegrasikan ekosistem alat mulai dari SIEM open source (Wazuh), DSPM/DLP komersial (BigID, Purview), hingga intelijen dark web (DarkRadar.io), dengan sorotan pada **Cyber Rank** sebagai jangkar *compliance* kontekstual Indonesia. Dengan pendekatan *end-to-end* (discover → classify → protect → detect → respond → report), buku ini menekankan bahwa **kepatuhan tidak sekadar formalitas**, tetapi instrumen strategis untuk membangun kepercayaan, mengurangi *mean time to detect/respond (MTTD/MTTR)*, sekaligus menekan potensi denda hingga **2% revenue tahunan** sesuai UU PDP.

Daftar Isi

Lisensi.....	2
Disclaimer.....	2
Executive Summary.....	3
Daftar Isi.....	4
Kata Pengantar.....	10
BAB 1: Pendahuluan.....	11
Latar Belakang.....	11
Tren Insiden Kebocoran Data & Tuntutan Regulasi.....	11
UU No. 27/2022 (UU PDP) & Masa Berlaku Penuh.....	12
Konsekuensi Legal dari Data Breach.....	12
Keterkaitan Narasi dengan Struktur Buku Anda.....	13
Tujuan Buku.....	14
Apa yang Dibimbing Buku Ini (Outcome yang Terukur).....	14
Cara Buku Ini Membimbing Praktek Lapangan.....	15
Bagaimana Pembaca Menggunakan Buku Ini.....	16
Kenapa Ini Mendesak—Data & Regulasi Menopang Argumen.....	16
Lingkup.....	16
Automated Checks (continuous, evidence-ready).....	16
Data Leak Detection (SaaS/Email/Code/File-share).....	17
Dark-Web Monitoring (domain/email/brand/exec).....	17
Automatic Remediation / Advice (SOAR-centric).....	18
Cakupan Lingkungan.....	18
Output yang Diwajibkan (siap audit UU PDP).....	19
Ringkasnya.....	19
BAB 2: Kerangka UU PDP untuk Praktisi Teknis.....	20
Prinsip & Pasal Kunci (ringkas untuk engineer).....	20
1. Hak Subjek Data → user-facing workflows wajib ada.....	20
2. Dasar Hukum (Lawful Basis) & Prinsip Pemrosesan.....	20
3. Pengendali vs Prosesor → RACI & kontrak vendor.....	20
4. Keamanan Pemrosesan → controls & evidence.....	21
5. DPIA (Data Protection Impact Assessment) → gating control untuk high-risk processing.....	21
6. Pencatatan Aktivitas Pemrosesan (ROPA).....	21
7. Penghapusan/Pemusnahan & Retensi.....	21
8. Notifikasi Insiden (Breach Notification) → ≤ 3×24 jam.....	21
9. Transfer Data ke Luar Negeri (Cross-Border Transfer).....	22
10. Sanksi & Penegakan → desain kontrol yang audit-ready.....	22
“Engineer Cheat-Sheet”: Pasal → Kontrol → Bukti (contoh cepat).....	22
Kenapa ini krusial untuk tim teknis (data & tren singkat).....	22
Ringkasnya.....	22
Peran Pengendali vs Prosesor Data.....	23

1. Pengendali Data (Data Controller).....	23
2. Prosesor Data (Data Processor).....	23
3. Statistik Risiko & Realitas Vendor.....	24
4. Titik Kontrol Teknis (Controller ↔ Processor).....	24
5. Implikasi UU PDP: Siapa Bertanggung Jawab?.....	24
Ringkas untuk Engineer.....	24
Tabel Perbandingan Peran Pengendali vs Prosesor Data (UU PDP).....	25
Contoh DPA Policy-as-Code (YAML).....	26
Contoh DPA Policy-as-Code (JSON).....	27
Kewajiban Keamanan & Pemberitahuan Insiden.....	29
1. Kewajiban Keamanan (Security of Processing).....	29
2. Pemberitahuan Insiden (Breach Notification).....	29
3. Konsekuensi Jika Gagal.....	30
4. Rekomendasi Teknis untuk Engineer.....	30
Template Notifikasi Insiden – Regulator.....	31
Template Notifikasi Insiden – Publik (Subjek Data).....	32
Mapping UU PDP ↔ Kontrol Teknis.....	33
1. Data Minimization (Pasal 17–22).....	33
2. Lawful Basis & Consent (Pasal 20–23).....	33
3. Security of Processing (Pasal 39).....	33
4. Data Protection Impact Assessment (DPIA) (Pasal 34).....	33
5. Rights of Data Subject (Pasal 5–13).....	34
6. Statistik Penting (2023–2024).....	34
7. Mengapa Mapping Penting?.....	34
BAB 3: Metodologi Audit & Skema Penilaian Tools.....	35
Tahap Audit.....	35
1. Discover — tahu di mana PII berada.....	35
2. Classify — tahu apa yang sensitif.....	35
3. Protect — cegah eksposur sejak desain.....	35
4. Detect — temukan lebih cepat dari penyerang.....	36
5. Respond — ubah alert jadi aksi otomatis.....	36
6. Report — bukti siap audit & learning loop.....	36
Kenapa Siklus Ini Mendesak — Reality Check.....	37
Ops Guide singkat per tahap (siap dioperasikan).....	37
Ringkasnya.....	37
Checklist Teknis per Tahap Audit.....	37
1. Discover.....	37
2. Classify.....	38
3. Protect.....	38
4. Detect.....	38
5. Respond.....	39
6. Report.....	39
Contoh Policy-as-Code.....	40
A. Public-Link Kill-Switch (SaaS/Cloud Drive).....	40

B. Auto-Notice Generator (UU PDP – ke Regulator & Publik).....	40
Kriteria Evaluasi (Skor 1–5).....	41
1. Automated Privacy Audit.....	41
2. Data Leak Detection (SaaS/Email/Repo/File Share).....	42
3. Password Leak Check.....	42
4. Sensitive-Info Leak (Regex/ML).....	42
5. Dark Web Monitoring.....	42
6. Automatic Advice & Remediation (SOAR/Playbooks).....	43
7. Compliance & Reporting (UU PDP/ISO/GDPR).....	43
8. Integrasi & Operasional (SIEM, Ticketing, False Positive Mgmt).....	43
9. Biaya & TCO (Total Cost of Ownership).....	43
Tabel Rubrik Skoring Audit Data Privacy (UU PDP).....	44
Bobot Rekomendasi.....	46
1. Dimensi Teknis (40%).....	46
2. Dimensi Kepatuhan (25%).....	46
3. Dimensi Otomasi (20%).....	47
4. Dimensi TCO (15%).....	47
Kesimpulan Praktis.....	47
BAB 4: Pemetaan Kontrol: Dari UU PDP ke Fitur Tool.....	48
Matriks Pasal/Prinsip ↔ Kontrol ↔ Artefak Bukti.....	48
Matriks Pasal/Prinsip ↔ Kontrol ↔ Artefak Bukti.....	48
Contoh “Security of Processing” → kontrol → bukti (diperluas).....	50
Format artefak bukti (audit-ready checklist).....	50
Tabel Pemetaan UU PDP → Kontrol Teknis → Artefak Bukti → KPI.....	51
Contoh YAML Policy-as-Code.....	52
1. Public Link Kill-Switch (M365/GDrive/SharePoint).....	52
2. Auto-Notice Generator (Breach Detection → Notifikasi 3×24 jam).....	53
Ringkasan eksekutif (untuk manajemen).....	53
BAB 5: Cyber Rank untuk Audit Data Privacy & Vendor Risk Management.....	54
Kasus Penggunaan.....	54
1. Due Diligence Vendor (pra-kontrak).....	54
2. Pemantauan Berkala Third-Party (pasca-onboarding).....	55
“What good looks like”.....	56
Nilai terdiferensiasi Cyber Rank (vs pasar).....	56
Output & Bukti Audit.....	57
1. Laporan Skor Risiko Vendor (Vendor Risk Score).....	57
2. Temuan Privasi (Privacy Findings).....	57
3. Remediation Tracker (SLA & Ownership).....	58
4. Evidence Pack (Siap Audit).....	58
5. Integrasi & Operasionalisasi (GRC/SIEM/SOAR/Procurement).....	58
6. Daftar Bukti (Ringkas, siap ditempel ke checklist audit).....	59
7. Dampak ke UU PDP (penekanan operasional).....	59
Integrasi.....	59
Kelebihan & Keterbatasan.....	59

Checklist Implementasi Cepat (4 Minggu).....	60
Kesimpulan.....	60
BAB 6: DarkRadar.io Threat Intelligence.....	61
Fitur Inti & Fungsi Operasional.....	61
Kasus Penggunaan / Use Cases Kritis.....	62
Integrasi & Otomasi di Arsitektur Keamanan.....	63
Output & Bukti Audit.....	64
Kelebihan & Keterbatasan (Analisis Kritis).....	64
Playbook Respons 24 Jam (Contoh Langkah-demi-langkah).....	65
Posisi DarkRadar.io dalam Lanskap Tool dalam Buku Ini.....	66
Catatan Penutup & Rekomendasi untuk Praktisi IT.....	66
BAB 7: Panorama Pasar: Privacy/DSPM/DLP, OSS, OSINT & Identity Exposure.....	68
Snapshot Eksekutif (apa yang penting untuk IPT/IT Ops).....	68
Commercial Privacy/DSPM/DLP.....	68
OneTrust (PrivacyOps & Data Mapping).....	68
BigID (DSPM/Data Discovery).....	68
Securiti.ai (Data Command Center / DSPM).....	68
Microsoft Purview (DLP di M365/Windows/Endpoint).....	69
Google Cloud DLP / Sensitive Data Protection.....	69
Symantec DLP (Broadcom).....	69
Open-Source / Community.....	69
Wazuh (XDR/SIEM) + Suricata (NIDS/NIPS/NSM).....	69
TruffleHog / Gitleaks (Secrets & Repo Leaks).....	70
OSINT Dark-Web & Otomasi.....	70
Ahmia & OnionScan.....	70
n8n (Workflow/Otomasi).....	70
Identity Exposure (Password/Kredensial).....	70
Have I Been Pwned (HIBP).....	70
SpyCloud.....	70
Pemetaan Singkat ke UU PDP (apa yang jadi artefak?).....	71
Catatan Kritis & Rekomendasi Implementasi.....	71
Daftar Sumber Kunci (untuk due diligence cepat).....	72
Bonus ringkas (untuk slide).....	72
BAB 8: Perbandingan Tools.....	73
Cyber Rank – Fokus Compliance dan Vendor Risk.....	73
DarkRadar.io – Early Warning Dark-Web & Breach Intel.....	73
BigID / Securiti – DSPM & DLP Premium.....	74
Wazuh – OSS SIEM Fleksibel.....	74
TruffleHog & Gitleaks – Secrets Scanner untuk DevSecOps.....	75
Ringkasan Eksekutif.....	75
BAB 9: Arsitektur Integrasi & Otomasi (SOAR-Centric).....	76
Referensi Arsitektur (Sinyal → Korelasi → Aksi).....	76
Peran Khusus Cyber Rank (jangkar kepatuhan UU PDP).....	76
Playbook Kunci (SOAR-first).....	77

A. Public-link PII exposure (M365/Google Drive).....	77
B. Employee credential exposure terdeteksi DarkRadar.io / HIBP.....	77
C. PII in Git (TruffleHog/Gitleaks).....	77
Paket Bukti Audit Otomatis (untuk UU PDP).....	78
Tantangan yang Harus Diantisipasi.....	78
Pola Implementasi (ringkas).....	78
Key Takeaways.....	79
BAB 10: Studi Kasus (Indonesia-centric).....	80
Studi Kasus 1: Pemda/RS Pendidikan – Budget Ketat, Fokus OSS dan Low-Cost Compliance.....	80
Studi Kasus 2: Startup Fintech – Kecepatan & Cloud, Prioritas Agility di Tengah Boom Digital.....	81
Studi Kasus 3: Enterprise Multinasional – Multi-Regulasi, Fokus Skalabilitas Global-Lokal	81
BAB 11: Roadmap Implementasi (12 Minggu).....	83
Minggu 1–2: Gap Assessment PDP, Data Flow Mapping, dan Tool Shortlist.....	83
Minggu 3–4: Pilot Cyber Rank + DarkRadar.io + 1 DSPM/DLP.....	84
Minggu 5–6: Integrasi SIEM/SOAR; Rancang 3 Playbook Prioritas.....	84
Minggu 7–8: UAT, Simulasi Table-Top, Ukur MTDD/MTTR.....	84
Minggu 9–12: Rollout Bertahap; Metrics & Executive Dashboard.....	85
BAB 12: Analisis & Rekomendasi Akhir.....	86
Pilar Rekomendasi Utama.....	86
Kombinasi Optimal Berdasarkan Skala.....	86
Rekomendasi Eksekutif.....	87
Kesimpulan Kritis.....	87
Kesimpulan.....	88
Posisi Strategis Tiap Tools.....	88
Rekomendasi Kombinasi Optimal.....	89
Penutup Kritis.....	89
Lampiran A: Rubrik Skoring (1–5 per Kriteria).....	90
Contoh Skor Evaluasi Tools.....	92
Tabel Skor Tools (1–5).....	92
Interpretasi Hasil.....	93
Lampiran B: Template Evidence Pack (log, tiket, laporan insiden).....	94
Lampiran C: Regex/Detector contoh (NIK, NPWP, CC, medis) & masking script.....	98
Statistik & Urgensi.....	98
Contoh Regex Detector.....	98
Masking Script (Python/Pandas contoh).....	99
Peran Cyber Rank.....	99
Rekomendasi Implementasi.....	99
Lampiran D: Sample dokumen kebijakan & SOP insiden (UU PDP).....	101
Konteks Strategis.....	101
Statistik & Realitas Lapangan.....	101
Struktur Dokumen Kebijakan (Sample).....	101
SOP Insiden (Template Flow).....	102

Peran Cyber Rank.....	102
Rekomendasi Implementasi.....	102
Lampiran E: Glosarium.....	104
Cara Pakai.....	104
A. Hukum & Tata Kelola (UU PDP & turunan teknis).....	104
B. Data & Proteksi (konsep inti untuk engineer).....	105
C. Deteksi, Respons, & Intel.....	105
D. Operasionalisasi & Bukti.....	106
E. Vendor / Supply-Chain.....	106
F. Istilah Teknis Pelengkap (ringkas cepat).....	107
Penutup (Operasional & Audit).....	107
LAMPIRAN F: Kerangka Tabel “Executive One-Pager”	108
Tentang Penulis.....	109

Kata Pengantar

Di tengah meningkatnya insiden kebocoran data — **94,22 juta akun penduduk Indonesia terekspos antara 2020–2023** menurut Kominfo & BSSN — kebutuhan akan panduan praktis untuk *compliance* dengan **UU No. 27/2022 (UU PDP)** menjadi semakin mendesak. Buku ini disusun bukan sekadar sebagai literatur akademik, melainkan sebagai **toolkit operasional** bagi praktisi IT, auditor, dan manajemen risiko yang berhadapan langsung dengan tantangan regulasi dan realitas teknis di lapangan.

Pendekatan kami menekankan tiga hal:

1. **Keterhubungan regulasi dengan kontrol teknis** melalui pemetaan *Pasal ↔ kontrol ↔ bukti audit*;
2. **Integrasi otomatisasi** menggunakan *automated privacy audit, leak detection, dark-web monitoring, hingga SOAR playbook*;
3. **Relevansi kontekstual Indonesia**, dengan menempatkan **Cyber Rank** sebagai jangkar utama *compliance* vendor/third-party, sekaligus menyoroti DarkRadar.io, BigID/Securiti, Wazuh, hingga OSS tools seperti TruffleHog.

Novelty buku ini adalah menjembatani *compliance gap*: dari pasal hukum yang abstrak menuju **artefak teknis siap audit** (policy, log, report, ticket). Dengan demikian, buku ini diharapkan tidak hanya mempercepat adopsi kepatuhan UU PDP, tetapi juga menurunkan *Mean Time to Detect/Respond (MTTD/MTTR)* insiden, serta mitigasi potensi sanksi administratif hingga **2% dari revenue tahunan** bagi organisasi yang lalai.

Singkatnya, **Kata Pengantar** ini menegaskan misi: menghadirkan panduan **tajam, operasional, dan kontekstual** yang dapat langsung dipakai untuk membangun *privacy resilience* Indonesia di era digital.

Jakarta, September 2025

Onno W. Purbo

BAB 1: Pendahuluan

Latar Belakang

Transformasi digital di Indonesia berkembang pesat: jumlah pengguna internet terus meningkat (misalnya survei menunjukkan pertumbuhan ke 221,5 juta pengguna di tahun 2023—dari 204,7 juta di 2022) ([ResearchGate](#)). Namun, percepatan digitalisasi juga membawa **eksposur risiko proteksi data pribadi** yang semakin tinggi.

Beberapa catatan penting:

- Dalam kurun waktu **empat tahun terakhir**, sekitar **94,22 juta akun** data penduduk Indonesia telah dilaporkan bocor — menjadikan Indonesia sebagai salah satu negara dengan kebocoran data terbanyak secara global. ([CSIRT Indonesia](#))
- Di peringkat dunia, Indonesia berada di urutan ke-8 dalam hal besar jumlah akun yang bocor sepanjang periode 2020–2024 ($\approx 94,22$ juta) ([Databoks](#))
- Insiden siber “multi-agency” turut memberi gambaran risiko pada tingkat negara: lebih dari **40 lembaga pemerintah** terkena serangan ransomware yang mengganggu layanan imigrasi dan operasi bandara, dengan permintaan tebusan US\$ 8 juta oleh kelompok *LockBit 3.0* ([Reuters](#))
- Laporan ancaman juga menunjukkan Indonesia menghadapi **4.046 serangan phishing** dalam periode tertentu, dan **43.879 insiden DDoS**, dengan serangan puncak hingga 693 Gbps bandwidth, mengindikasikan betapa intensnya ancaman siber di ranah data/komunikasi. ([SocRadar](#))

Data ini menegaskan bahwa **insiden kebocoran data bukan lagi sekadar kemungkinan**, melainkan sesuatu yang hampir pasti akan dialami oleh organisasi yang mengelola data pribadi di Indonesia, kecuali mitigasi keamanan dijalankan dengan sangat kuat.

Tren Insiden Kebocoran Data & Tuntutan Regulasi

Seiring meningkatnya publisitas terhadap *data breaches*, ekspektasi terhadap regulasi dan penegakan hukum ikut naik. Beberapa dinamika yang patut dicermati:

- **Tuntutan regulasi lokal:** UU PDP (UU No. 27/2022) muncul sebagai jawaban atas kekosongan regulasi yang jelas terkait data pribadi di Indonesia.
- **Tekanan global & benchmarking GDPR:** banyak organisasi Indonesia mulai diukur terhadap standar internasional seperti GDPR, serta best practice internasional (misalnya *privacy by design*, *data minimization*).
- **Ekspektasi transparansi & akuntabilitas:** regulator, pemangku kepentingan, dan publik menuntut bahwa pengelolaan data bukan “kotak hitam” — organisasi harus menunjukkan bahwa mereka memiliki kontrol teknis dan bukti audit yang dapat diaudit.
- **Peningkatan litigator & gugatan perdata:** persoalan data bocor tidak hanya soal hukuman negara, tetapi juga potensi **gugatan massal** (class action) dari para subjek data yang dirugikan.

Tren ini mengubah lanskap: bukan lagi pertanyaan “**apakah ada kebocoran?**”, tapi “**seberapa cepat dan bagaimana respons Anda?**”

UU No. 27/2022 (UU PDP) & Masa Berlaku Penuh

UU PDP disahkan pada 17 Oktober 2022. Ia menawarkan kerangka hukum baru untuk proteksi data pribadi di Indonesia. Beberapa poin penting:

- **Masa transisi:** UU PDP memberikan masa transisi agar entitas mengadaptasi regulasi ini. Transisi ini akhirnya berakhir, dan **kepatuhan penuh (full enforcement)** diwajibkan.
- **Pasal sanksi & pidana:**
 - Pasal 65–68 mengatur pidana bagi individu yang memperoleh, mengungkapkan, atau menggunakan data pribadi yang bukan miliknya. Misalnya: pidana maksimal **5 tahun penjara dan/atau denda hingga Rp 5 miliar** untuk pengumpulan/ penggunaan data pribadi milik orang lain. ([JDIH Kemkomdigi](#))
 - Pasal 68 mengatur pemalsuan data pribadi: pidana hingga **6 tahun dan/atau denda hingga Rp 6 miliar**. ([JDIH Kemkomdigi](#))
 - Pasal 57 menyebutkan **sanksi administratif**, termasuk denda hingga **2 % dari pendapatan tahunan** organisasi, penghentian sementara pemrosesan data, penghapusan data, dan/atau pencabutan izin. ([Peraturan BPK](#))
 - Untuk korporasi, Pasal 70 memperbolehkan pidana tambahan: misalnya **10 kali lipat denda kriminal**, pembekuan usaha, pencabutan izin, hingga pembubaran. ([JDIH Kemkomdigi](#))
 - Dalam pelaksanaan, tantangan muncul terkait pembuktian kesalahan, kelalaian, niat jahat, serta ketersediaan data bukti digital (forensik) yang memadai. ([Hukumonline](#))

Dengan berakhirnya masa transisi, **setiap organisasi yang memproses data pribadi di Indonesia kini sepenuhnya tunduk UU PDP**—tidak lagi ada alasan “belum siap” sebagai pembelaan.

Konsekuensi Legal dari Data Breach

Ketika terjadi **kebocoran data (data breach)** — baik karena serangan eksternal, kesalahan konfigurasi, vendor lemah, human error, atau kombinasi — organisasimu menghadapi risiko hukum yang nyata dan multi-dimensi:

1. Sanksi administratif (regulator)

- **Peringatan tertulis**
- **Penghentian sementara aktivitas pemrosesan data**
- **Penghapusan atau pemusnahan data**
- **Denda administratif hingga 2 % dari pendapatan tahunan** sesuai jenis dan besaran pelanggaran (Pasal 57 UU PDP) ([Peraturan BPK](#))

2. Sanksi pidana (individu / korporasi)

- Untuk individu yang secara sengaja memperoleh, mengungkapkan, atau menggunakan data pribadi milik orang lain: pidana hingga **5 tahun dan/atau denda hingga Rp 5 miliar** ([JDIH Kemkomdigi](#))
- Untuk pemalsuan data: pidana maksimal **6 tahun dan/atau denda hingga Rp 6 miliar** ([JDIH Kemkomdigi](#))
- Untuk korporasi: denda kriminal dapat ditingkatkan **10 kali lipat**, ditambah pidana tambahan (pembekuan usaha, pencabutan izin, pembubaran) ([JDIH Kemkomdigi](#))
- Pidana tambahan juga mencakup **perampasan keuntungan / aset hasil tindak pidana** dan **ganti kerugian** kepada subjek data. ([SIP Law Firm](#))

3. Litigasi perdata / ganti rugi oleh subjek data

- Subjek data yang dirugikan dapat mengajukan **gugatan perdata**, menuntut **ganti rugi material maupun immaterial**
- Bila terjadi kebocoran massal, potensi **class action** atau litigasi kolektif meningkat.
- Organisasi harus siap membuktikan bahwa mereka telah melaksanakan *due diligence*, kontrol teknis & organisasi yang memadai, serta respons insiden secara tepat waktu.

4. Reputasi & kepercayaan publik

- Kebocoran data sering kali menimbulkan krisis kepercayaan, kehilangan pelanggan atau pengguna, penurunan valuasi organisasi, dan dampak bisnis jangka panjang yang sulit diukur.
- Regulasi modern memandang reputasi sebagai “modal sosial” — kerusakan reputasi bisa menjadi pintu masuk tekanan audit, legislatif, dan pengawasan publik.

5. Biaya teknis & operasional tak terduga

- Investigasi forensik, remediasi, pemberitahuan wajib ke regulator & subjek data, litigasi, audit eksternal, dan penguatan ulang sistem — semua ini dapat menelan biaya yang jauh melebihi investasi keamanan proaktif.

Keterkaitan Narasi dengan Struktur Buku Anda

Narasi latar belakang yang kuat ini secara langsung mendasari BAB 1 buku Anda. Berikut cara integrasinya:

- Dalam BAB 1: narasi ini akan menjadi “Latar Belakang” + “Tren insiden & regulasi”
- Penekanan pada UU PDP dan konsekuensi legal menggiring motivasi kenapa “Audit Data Privacy berbasis tools & otomatisasi” menjadi **kebutuhan mutlak**, bukan sekadar “nice-to-have”
- Statistik & contoh nyata (misalnya bocornya 94 juta akun, serangan ransomware ke instansi pemerintah) bisa dijadikan *case hook* di awal buku untuk menggugah urgency.

- Narasi ini juga menyambung ke bagian-bagian teknis selanjutnya: pembaca IT akan lebih memahami bahwa pemetaan pasal → kontrol teknis bukan hiasan semata, melainkan tanggung jawab yang dapat diuji di pengadilan

Tujuan Buku

Buku ini ditulis sebagai **panduan praktis** bagi tim IT, *security engineering*, dan *data protection* untuk **melakukan audit privasi berbasis tools dan otomasi**—bukan sekadar kepatuhan di atas kertas. Targetnya: organisasi **mampu membuktikan** (1) bahwa kontrol teknis berjalan, (2) bahwa insiden dapat **dideteksi lebih cepat** dan **direspons lebih singkat**, serta (3) bahwa **artefak bukti** siap dipresentasikan ke manajemen dan regulator (UU PDP).

Kenapa fokus pada otomasi dan *tooling*?

- **Biaya insiden sangat material.** Rata-rata biaya *data breach* global dilaporkan **US\$ 4,88 juta** (periode 2023–2024), lalu **turun menjadi ~US\$ 4,4 juta pada 2025** seiring peningkatan **kecepatan identifikasi & containment**—indikasi bahwa investasi pada deteksi cepat dan respons terotomasi memang **menurunkan biaya**. ([ibm.com](https://www.ibm.com))
- **Vektor kredensial & dark web kian dominan.** Laporan 2024–2025 menunjukkan **eksposur kredensial** dan *data exposure alerts* di *dark web* meningkat (mis. **+15,4%** YoY menurut CRIF; jutaan kredensial terekspos menurut SOCRadar/SpyCloud). **Artinya, pemantauan external exposure harus jadi kapasitas inti**, bukan pelengkap. ([crif.com](https://www.crif.com))
- **Pola serangan tak lagi tunggal.** DBIR 2024 menegaskan kombinasi *phishing*, penyalahgunaan kredensial, dan *misconfiguration* mendominasi jalur menuju *breach*—mendorong kebutuhan *controls* yang saling terkait: DSPM/DLP, IAM/MFA/SSO, *cloud posture*, dan *automated response*. ([Verizon](https://www.verizon.com))
- **UU PDP sudah berlaku penuh.** Dengan **masa transisi selesai**, organisasi wajib dapat menunjukkan **keterpenuhan kewajiban**, termasuk **pemberitahuan insiden**, **keamanan pemrosesan**, dan kesiapan **sanksi administratif** (hingga **2% pendapatan**), pidana untuk pelanggaran tertentu, serta pidana tambahan untuk korporasi. **Membuktikan kontrol** lewat *scan report*, *incident ticket*, dan *evidence pack* bukan lagi *nice-to-have*. ([Peraturan BPK](https://peraturan.bpk.go.id))

Apa yang Dibimbing Buku Ini (Outcome yang Terukur)

1. **Audit yang bisa dijalankan mingguan/harian, otomatis.**
 - *Goal: Mean Time to Detect (MTTD)* dan *Mean Time to Respond (MTTR)* **turun signifikan** melalui *playbook* otomasi (*SOAR-style*) untuk kasus berulang (PII terbuka di *cloud drive*, kredensial bocor, *secrets* di repo).
 - *Kenapa otomasi?* Praktik industri menempatkan otomasi sebagai cara menaikkan skala operasi dan **memangkas MTTR** sehingga biaya insiden ikut turun. ([Palo Alto Networks](https://www.paloaltonetworks.com))

2. **Pemetaan pasal UU PDP → kontrol teknis → bukti audit.**
 - *Goal*: setiap kewajiban (mis. **security of processing**, notifikasi insiden, hak subjek data) dipetakan ke **kontrol** dan *tool*: *DSPM/DLP, IAM/MFA, encryption, EDR, SIEM, dark-web monitoring*; lalu diikat dengan **artefak bukti** yang konsisten (kebijakan, *scan result, alert, ticket, SOAR log*).
 - *Manfaat*: memudahkan **tanya-jawab regulator** dan *board review*.
3. **Perbandingan *tools* untuk deteksi, pencegahan, dan saran otomatis (opini berbasis kriteria).**
 - *Goal*: memilih kombinasi *tool* yang **paling efisien** untuk konteks Indonesia—**bukan yang paling ramai di pasar**.
 - *Fokus kategori*:
 - **Compliance/Third-Party**: *Cyber Rank* (membantu *due diligence* vendor & *evidence* kepatuhan lokal).
 - **Dark-Web Intel**: *DarkRadar.io* (peringatan dini paparan eksternal & kredensial).
 - **DSPM/DLP & Privacy Platforms**: *BigID/Securiti/OneTrust; cloud DLP* (*Purview/Google DLP/Symantec DLP*).
 - **OSS Stack**: *Wazuh+Suricata* (*SIEM/NIDS*), *TruffleHog/Gitleaks* (*secrets/repo*), *OSINT & workflow n8n*.
 - *Keluaran*: **tabel komparatif** (fitur inti, integrasi *SIEM/SOAR, compliance reporting*, estimasi biaya/tier) yang **langsung bisa dipakai tender/PAC**.

Cara Buku Ini Membimbing Praktek Lapangan

- **Kerangka kerja audit berulang** (*Discover → Classify → Protect → Detect → Respond → Report*), plus **rubrik skoring 1–5** per kriteria:
 - **Automated checks** (*scheduled scan*, cakupan konektor),
 - **Data leak detection** (*SaaS/email/code/file-share*),
 - **Password/credential leak check** (*breach DB*),
 - **Sensitive-info leak** (*NIK/NPWP/CC/medis; regex/ML*),
 - **Dark-web monitoring**,
 - **Automatic advice/remediation** (*playbook, SOAR*),
 - **Compliance & reporting** (*template UU PDP/ISO*),
 - **Integrasi & operasi** (*SIEM, tiket, false-positive mgmt*),
 - **Biaya & TCO** (*lisensi, infra, tim, dampak MTTR*).

-> **Bobot rekomendasi: Teknis 40% | Kepatuhan 25% | Otomasi 20% | TCO 15%** (*transparan, defensible* untuk keputusan manajemen).
- **Peta pasal UU PDP ke kontrol teknis (BAB 4)**:
 - Contoh: **Security of Processing → DLP/DSPM, CASB, EDR, IAM, encryption → bukti**: *policy, scan report, incident ticket, SOAR log*.
 - **Template Evidence Pack** agar setiap audit dapat **dibuktikan cepat**.

- **Arsitektur integrasi & otomasi (BAB 9):**
 - **Sinyal:** DSPM/DLP + DarkRadar.io + HIBP/SpyCloud + EDR
 - **Korelasi:** SIEM (Wazuh/Sentinel/Splunk)
 - **Aksi:** SOAR *playbooks* → *quarantine, revoke OAuth, reset password, notify DPO*
 - *Rasional industri:* otomasi dipakai untuk **mengurangi *alert fatigue*** dan **mempercepat penutupan insiden**, yang relevan langsung dengan biaya *breach*. ([Palo Alto Networks](#))

Bagaimana Pembaca Menggunakan Buku Ini

- **Sebagai *runbook* implementasi 12 minggu:** dari *gap assessment* → *pilot tools* (Cyber Rank + DarkRadar.io + 1 DSPM/DLP) → integrasi SIEM/SOAR → UAT/simulasi → *rollout* bertahap dengan **KPI MTTD/MTTR**.
- **Sebagai *decision brief*:** *executive one-pager* memuat 2–3 paket rekomendasi (skala kecil/menengah/besar) lengkap **estimasi biaya/tier & konsekuensi residual risk**.
- **Sebagai *audit aid*:** *checklist* bukti (log, tiket, laporan insiden, *DPIA* ringkas), siap dikirim ke **DPO, auditor internal, dan regulator** saat dibutuhkan di bawah rezim **UU PDP**. ([Peraturan BPK](#))

Kenapa Ini Mendesak—Data & Regulasi Menopang Argumen

- **Biaya *breach*** tinggi dan sensitif terhadap **kecepatan deteksi/response**—itulah justifikasi inti otomasi dan integrasi *tooling*. ([ibm.com](#))
- **Kredensial & *dark-web exposure*** melonjak; *tooling* yang **memantau eksternal + memicu tindakan otomatis** (reset, *revoke*) **bukan lagi opsional**. ([crif.com](#))
- **UU PDP berlaku penuh; sanksi administratif hingga 2% pendapatan** dan pidana untuk pelanggaran tertentu menuntut **kontrol yang bisa dibuktikan**, bukan sekadar SOP. ([Peraturan BPK](#))

Lingkup

Buku ini membatasi ruang kerja pada **empat fokus kontrol** yang paling berdampak terhadap **MTTD/MTTR** dan **pembuktian kepatuhan UU PDP**: (1) **automated checks**, (2) **data leak detection**, (3) ***dark-web monitoring***, dan (4) ***automatic remediation/advice***. Lingkup operasi mencakup **on-prem, cloud (IaaS/PaaS), SaaS, perangkat end-user**, serta **vendor/mitra (third-party)**—karena **68% breach melibatkan *human element***, dan **>1/3 breach** kini berakar dari pihak ketiga. **Artinya, otomasi *end-to-end* lintas perimeter dan rantai pasok bukan lagi opsional**. ([Verizon](#))

Automated Checks (continuous, evidence-ready)

Tujuan: memastikan **pemindaian terjadwal** dan **kontrol preventif/detektif** berjalan *by design*, menghasilkan **artefak bukti** (policy, scan report, tiket, *SOAR log*) yang siap audit.

- **Apa yang di-check:**

- *Cloud posture* (IaaS/PaaS), *SaaS misconfiguration*, eksposur *public link* (Drive/SharePoint), *PII discovery/classification* (DSPM/DLP), *secrets* di repos (CI/CD).
- *Identity posture* (MFA/SSO, *password policy*, *impossible travel*) dan *endpoint posture* (EDR/AV/patch level).
- **Kenapa kritikal:** **10.626 breach** tercatat di DBIR 2024 (rekor), *ransomware/extortion* ~32%, dan 68% melibatkan *human element*—indikasi kuat bahwa *misconfig*, kredensial lemah, dan proses manual perlu diganti **otomasi**. **Automated checks** menurunkan *dwell time* dan mempercepat *containment*. ([Skyhigh Security](#))
- **KPI contoh:** cakupan konektor ≥90% aset kritikal; *scan S3/Blob/Drive* harian; *secrets scan* setiap *push*; *policy drift* ≤24 jam.

Catatan biaya: Rata-rata biaya *data breach* global turun ~9% dari **US\$4,88M (2024)** menjadi ~**US\$4,44M (2025)**—ditopang **identifikasi & containment lebih cepat** melalui **AI & otomasi**. Ini memperkuat tesis investasi pada *automated checks*. ([bakerdonelson.com](#))

Data Leak Detection (SaaS/Email/Code/File-share)

Tujuan: mendeteksi **data/PII keluar jalur** di SaaS, email, *code repo*, dan *file-share* sebelum berdampak luas.

- **Ruang lingkup teknis:**
 - **SaaS:** *public link exposure* (Drive, SharePoint), *overshared folder*, *link-to-anyone*, *GenAI data egress*.
 - **Email/Collab:** *DLP policies* (PII/NIK/NPWP/CC/medis), *exfil via forwarding*.
 - **Code/CI-CD:** *secrets* (API key/token) via **TruffleHog/Gitleaks**.
 - **File-share:** SMB/NAS/SharePoint modern + *watermarking/tagging*.
- **Kenapa kritikal:** **Interaksi SaaS/cloud naik ~35% YoY**; *shadow-SaaS* dan *GenAI apps* mendongkrak permukaan serangan—mendorong kebutuhan **deteksi kebocoran di lapisan aplikasi**. ([Medium](#))
- **KPI contoh:** *time-to-revoke public link* ≤60 menit; *policy hit* sensitif <x/bulan; *secret leak mean time to fix* ≤1 hari.

Dark-Web Monitoring (domain/email/brand/exec)

Tujuan: peringatan dini atas **kredensial & artefak organisasi** yang beredar di *underground* (forum/market/chat).

- **Ruang lingkup teknis:** *domain/email watchlist*, *brand impersonation*, *supplier mentions*, **IOC feed** ke SIEM.
- **Kenapa kritikal:** Pada 2024, SpyCloud “**recaptured**” **53,3 miliar identity records** (+22% vs 2023). Riset juga menunjukkan **rataan individu terekspos punya 141 credential pairs**—cukup bagi pelaku untuk *stuffing/takeover* skala besar. **Artinya, dark-web intel + credential hygiene wajib berjalan rutin**. ([SpyCloud](#))
- **KPI contoh:** *time-to-reset akun terekspos* ≤30 menit, *token revoke* otomatis, *korelasi intel* → *auth logs* ≤15 menit.

Automatic Remediation / Advice (SOAR-centric)

Tujuan: konversi *alert* menjadi **aksi otomatis** yang **mengurangi MTTR** dan **menghasilkan bukti**.

- **Contoh *playbook* prioritas:**
 - **Kredensial bocor (dark-web hit)** → *force reset, revoke OAuth, invalidate refresh token, notify DPO + tiket insiden*.
 - **PII terpublikasi (M365/GDrive)** → *auto quarantine, ubah sharing policy, owner notify, re-scan folder*.
 - **Secret di repo** → *rotate key, create PR fix, block pipeline* sampai remedi selesai.
- **Mengapa wajib:** Otomasi respons dikaitkan dengan **pengurangan biaya breach** lewat siklus identifikasi-penanggulangan yang lebih singkat. **Tanpa otomasi, *alert fatigue* naik, insiden melebar.** (allcovered.com)
- **KPI contoh:** *MTTR P1 ≤4 jam, percent auto-closed insiden berulang ≥60%, audit-ready evidence ≤15 menit* pasca-aksi.

Cakupan Lingkungan

Kenapa cakupan harus holistik? Karena **serangan kini menembus rantai pasok: ~35,5% breach (2024) terkait third-party access**; beberapa sumber bahkan menilai ~30% menurut interpretasi DBIR terbaru. **Mengamankan *perimeter sendiri* tanpa memantau vendor/mitra sama saja meninggalkan pintu belakang terbuka.** ([SecurityScorecard](https://securityscorecard.com))

- **On-Prem**
 - **Fokus:** *asset discovery, EDR/NIDS, DLP endpoint, least privilege, backup/immutability*.
 - **Integrasi:** SIEM (Wazuh/Splunk/Sentinel), *ticketing, SOAR*.
- **Cloud (IaaS/PaaS)**
 - **Fokus:** *CSPM/CIEM, workload protection, encryption at rest/in transit, KMS hygiene, public object scan*.
 - **Integrasi:** *cloud logs* → SIEM; *IaC policy* (shift-left).
- **SaaS**
 - **Fokus:** *SSPM/DLP SaaS, public link control, tenant-to-tenant sharing, GenAI egress guardrails*. **Interaksi SaaS ↑ ~35%** → deteksi eksposur jadi *must-have*. ([Medium](https://medium.com))
- **Perangkat End-User**
 - **Fokus:** *EDR/EPP, disk encryption, USB control, email DLP, browser isolation*.
 - **Rasional:** **68% breach melibatkan manusia** (phishing/cred reuse/mis-send) → kontrol di endpoint tak bisa dinego. ([Verizon](https://verizon.com))

- **Vendor/Mitra (Third-Party)**
 - **Fokus:** *external risk rating, questionnaire attestations, evidence sampling, contractual controls* (notifikasi insiden, *right to audit*), dan **pemantauan berkelanjutan**.
 - **Rasional:** **≥35,5% breach** berawal dari vendor; *supply-chain* jadi vektor yang paling sering dieksploitasi. ([SecurityScorecard](#))

Output yang Diwajibkan (siapa audit UU PDP)

- **Paket bukti otomatis** per insiden/kontrol: *scan report, alert context, who/what/when, playbook run logs, affected subject estimate, notifikasi DPO/regulator*.
- **Matriks pasal UU PDP** → kontrol → artefak (mis. **Security of Processing** → **DLP/DSPM/IAM/EDR/Encryption** → policy, hasil scan, tiket, **SOAR log**).
- **Dashboard eksekutif:** tren MTDD/MTTR, coverage, auto-remediation rate, third-party risk.

Ringkasnya

- **Fokus kita empat hal:** **automated checks, data leak detection, dark-web monitoring, automatic remediation/advice**.
- **Cakupan meliputi on-prem** → cloud → **SaaS** → endpoint → vendor.
- **Alasan bisnis & regulasi kuat:** biaya breach turun saat deteksi & respons dipercepat; **68% breach** masih berawal dari manusia; **≥35,5%** kini datang dari **third-party**—semuanya menuntut **otomasi lintas perimeter** yang **audit-ready**. ([bakerdonelson.com](#))

BAB 2: Kerangka UU PDP untuk Praktisi Teknis

Prinsip & Pasal Kunci (ringkas untuk engineer)

Tujuan ringkas bagian ini: memberi **peta minimal** yang bisa diterjemahkan langsung menjadi **kontrol teknis, log bukti, dan *playbook***. Fokus ke hal yang *actionable* bagi tim IT/SecEng/Privacy.

1. Hak Subjek Data → user-facing workflows wajib ada

- **Ruang lingkup pasal: Pasal 5–13** UU PDP mengatur hak akses, perbaikan, penghapusan, keberatan, pembatasan, portabilitas, dan penarikan persetujuan; **pengecualian** diatur di **Pasal 15**. **Implementasi:** formulir/self-service portal + SLA + *audit trail* (ROPA/ticket). (gerbangpelindungandatapribadi.id)
- **Kewajiban *timing* internal:** penarikan persetujuan → **hentikan pemrosesan ≤ 3×24 jam** sejak permohonan diterima (praktik implementasi yang dirujuk oleh ringkasan regulasi). **Kontrol teknis:** *consent registry, purpose binding, revocation hooks* di IAM/DLP. ([Ortax Data Center](https://ortaxdatacenter.com))

2. Dasar Hukum (Lawful Basis) & Prinsip Pemrosesan

- **Prinsip pemrosesan dan dasar hukum** berada di bab pemrosesan (lihat **Pasal 17–22** konteks UU); organisasi **wajib punya dasar pemrosesan** (mis. persetujuan, kontrak, kewajiban hukum, kepentingan vital/umum). **Kontrol teknis:** *purpose tag* di *data catalog*, *policy engine* untuk *least privilege*, *data minimization* dan *retention*. (sarolangunkab.go.id)
- **Angka pendukung risiko:** DBIR 2024 mencatat **10.626 breach (rekor)**; **68%** melibatkan *human element* (phishing/cred reuse/mis-send). Prinsip **minimisasi data + *strong auth* + *segregation*** adalah *must-have*. ([Peraturan BPK](https://peraturan.bpk.go.id))

3. Pengendali vs Prosesor → RACI & kontrak vendor

- **Definisi & perbedaan peran** diatur dan dijabarkan praktis oleh Hukumonline; **kewajiban pengendali** memproses berdasar persetujuan, membuktikan dasar hukum, dan memastikan prosesor patuh. **Kontrol:** *RACI matrix*, *DPA* (Data Processing Agreement), *right-to-audit*, *security addendum*. ([Hukumonline](https://hukumonline.com))
- **Kewajiban menunjuk petugas/pejabat PDP (setara *DPO*) (Pasal 53)** jika memenuhi kriteria (pelayanan publik, *large-scale monitoring*, atau pemrosesan skala besar data spesifik/kriminal). **Kontrol:** TOR peran, jalur pelaporan ke manajemen, *compliance dashboard*. ([Mahkamah Konstitusi RI](https://mahkamahkonstitusi.go.id))

4. Keamanan Pemrosesan → controls & evidence

- **Kewajiban keamanan** (mis. *state of the art* kontrol, pencegahan, *logging*) ditegaskan; **Pasal 39(2)** menekankan pencegahan menggunakan **sistem keamanan** yang memadai. **Kontrol:** *encryption at rest/in transit*, IAM/MFA/SSO, EDR/AV, *backup immutability*, SIEM, DLP/DSPM, *zero trust*. **Evidence:** *scan reports*, konfigurasi, *alert context*, *SOAR logs*. (icca.or.id)
- **Angka pendukung:** kombinasi konfigurasi salah + kredensial lemah mendominasi jalur *breach* (DBIR 2024); penguatan IAM/DLP/DSPM menurunkan *dwell time* dan biaya insiden. (icca.or.id)

5. DPIA (Data Protection Impact Assessment) → gating control untuk high-risk processing

- **Pasal 34** mewajibkan **Penilaian Dampak PDP (DPIA)** bila pemrosesan **berisiko tinggi** (mis. keputusan otomatis berdampak hukum signifikan, data spesifik dalam skala besar). **Kontrol:** *DPIA template*, *risk register*, *mitigation plan*, *sign-off* DPO. **Bukti:** dokumen DPIA, *residual risk acceptance*. (learning.hukumonline.com)

6. Pencatatan Aktivitas Pemrosesan (ROPA)

- Praktik kepatuhan merujuk **kewajiban pencatatan aktivitas pemrosesan (ROPA)** sehingga setiap *purpose*, *system of record*, dan *data flow* terdokumentasi. **Kontrol:** *data inventory* + *system registry* + *processor registry*. (privasimu.com)

7. Penghapusan/Pemusnahan & Retensi

- **Hak untuk penghapusan & pemusnahan** diatur (pengakhiran bila tujuan tercapai/retensi habis/permintaan subjek data). **Kontrol:** *retention scheduler*, *legal hold*, *crypto-shred*, *certificate of destruction*. ([Ortax Data Center](https://ortaxdatacenter.com))

8. Notifikasi Insiden (Breach Notification) → ≤ 3×24 jam

- **Kewajiban utama untuk engineer:** **bila terjadi “kegagalan perlindungan data pribadi”, pengendali Wajib memberi notifikasi tertulis kepada subjek data & lembaga **paling lambat **3×24 jam** (**Pasal 46** – redaksi dan rujukan *practice note*). **Kontrol:** *breach runbook*, *notice generator*, *contact data lake*, *timer SLA*. (learning.hukumonline.com)
- **Isi minimal notifikasi:** jenis data yang terungkap, kapan & bagaimana, serta langkah penanganan/pemulihan. **Kontrol:** *incident timeline auto-export* dari SIEM/SOAR. ([Ortax Data Center](https://ortaxdatacenter.com))

9. Transfer Data ke Luar Negeri (Cross-Border Transfer)

- **Pasal 56: wajib memastikan tingkat perlindungan setara/lebih tinggi** di negara tujuan (atau mekanisme yang diakui). **Kontrol:** *transfer risk assessment, SCC-like clauses*, lokasi data center/geo-fencing. ([JDIH Kemkomdigi](#))

10. Sanksi & Penegakan → desain kontrol yang audit-ready

- **Sanksi administratif** termasuk **denda hingga 2% pendapatan tahunan**, penghentian sementara pemrosesan, penghapusan/pemusnahan data, & pencabutan izin. **Implikasi teknis:** semua kontrol harus **punya bukti jalan** (log, tiket, scan report). ([Peraturan BPK](#))
- **Pidana & pidana tambahan untuk korporasi** (mis. denda dapat **×10** untuk korporasi, pembekuan usaha/pencabutan izin) mengharuskan **traceability penuh**: *who/what/when* untuk setiap keputusan teknis. ([JDIH Kemkomdigi](#))

“Engineer Cheat-Sheet”: Pasal → Kontrol → Bukti (contoh cepat)

- **Hak Akses/Perbaikan/Penghapusan (Pasal 5–13)** → *Subject Rights Portal, data subject search, redaction/masking* → **ticket + SLA log**. ([gerbangpelindungandatapribadi.id](#))
- **DPIA (Pasal 34)** → *risk scoring engine, auto-mitigation checklists* → **DPIA PDF + approval trail**. ([learning.hukumonline.com](#))
- **Keamanan Pemrosesan (Pasal 39(2))** → *encryption, EDR, IAM/MFA, DLP/DSPM, CSPM/CIEM* → **config snapshot, scan report, alert metrics**. ([icca.or.id](#))
- **Notifikasi Insiden ≤ 72 jam (Pasal 46)** → *SOAR playbook (classify impact → notify DPO → draft notice → dispatch)* → **incident timeline, copy surat, daftar subjek terdampak**. ([learning.hukumonline.com](#))
- **Cross-Border (Pasal 56)** → *geo-restriction, DPA clauses, transfer risk assess* → **legal memo + vendor assurances**. ([JDIH Kemkomdigi](#))

Kenapa ini krusial untuk tim teknis (data & tren singkat)

- **Skala ancaman:** DBIR 2024: **10.626 breach**, **68%** melibatkan manusia; *third-party* menjadi vektor signifikan → **otomasi + evidence by design** jadi prioritas. ([Peraturan BPK](#))
- **Efek pada biaya:** percepatan identifikasi/containment lewat otomasi & AI **menurunkan biaya breach** (tren 2024→2025). **Artinya, investasi di *pipeline evidence + playbook* bukan *cost center*, tapi **risk-adjusted savings**. ([jurnal.uia.ac.id](#))

Ringkasnya

- **Tujuh pilar operasional** untuk engineer: **Hak Subjek, Lawful Basis & Prinsip, Controller vs Processor & DPO, Keamanan Pemrosesan, DPIA, Retensi/Pemusnahan, Breach Notice 3×24 jam**, plus **Cross-Border**
- **Terjemahan teknisnya:** *policy-as-code, scan terjadwal, SOAR playbooks, subject-rights portal, transfer assessment*, dan **evidence pack** yang siap audit.

- **KPI wajib:** *coverage* kontrol, *SLA subject rights*, **MTTD/MTTR**, persentase *auto-remediate*, dan **ketepatan *breach notice* ≤ 72 jam**.

Peran Pengendali vs Prosesor Data

Dalam **UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)**, perbedaan antara **Pengendali Data** (*Data Controller*) dan **Prosesor Data** (*Data Processor*) menjadi fondasi tanggung jawab hukum. Untuk tim IT dan *engineer*, pemahaman ini penting karena berimplikasi langsung pada **arsitektur sistem**, **kontrak vendor**, dan **bukti audit**.

1. Pengendali Data (Data Controller)

- **Definisi:** Pihak yang menentukan tujuan (*purpose*) dan cara (*means*) pemrosesan data pribadi.
- **Contoh:** Bank yang mengelola data nasabah, rumah sakit yang menyimpan rekam medis, *e-commerce* yang mengelola data pelanggan.
- **Kewajiban kunci:**
 - Memastikan setiap pemrosesan punya **dasar hukum** (*lawful basis*) → misalnya persetujuan, kewajiban kontrak, kepentingan hukum.
 - Menjamin **keamanan pemrosesan** sesuai Pasal 39(2), dengan standar “state of the art” (enkripsi, IAM, DLP, SIEM).
 - **Notifikasi insiden** kepada regulator & subjek data paling lambat **3×24 jam** (Pasal 46).
 - Menunjuk **Petugas Perlindungan Data Pribadi (DPO)** bila skala risiko tinggi (Pasal 53).

Implikasi teknis:

- Harus punya *end-to-end visibility* atas semua aset data.
- Wajib memastikan *vendor & prosesor* patuh, dengan klausul *data processing agreement* (DPA).
- Audit evidence harus tersedia *on-demand* (scan report, policy config, incident ticket).

2. Prosesor Data (Data Processor)

- **Definisi:** Pihak yang memproses data pribadi **atas nama pengendali** sesuai instruksi kontrak.
- **Contoh:** Penyedia cloud (IaaS, SaaS), perusahaan outsourcing payroll, *managed security service provider* (MSSP).
- **Kewajiban kunci:**
 - Hanya memproses data sesuai instruksi pengendali.
 - Menyediakan **jaminan keamanan teknis & organisasi** (ISO/IEC 27001, log forensik, laporan audit).
 - Membantu pengendali memenuhi kewajiban **hak subjek data** (misalnya *erasure request* atau portabilitas).

Implikasi teknis:

- Harus punya *logging & monitoring* granular (akses, modifikasi, transfer data).
- Harus siap menyediakan **evidence pack** saat diminta pengendali.
- SLA keamanan wajib dipatok dalam kontrak (mis. MTTR, *breach notice* ≤ 24 jam ke pengendali).

3. Statistik Risiko & Realitas Vendor

- **~35,5% insiden kebocoran data global 2024** melibatkan pihak ketiga/vendor dalam rantai pasok. Supply-chain attack menjadi jalur populer bagi penyerang.
- Di Indonesia, **lebih dari 94 juta akun bocor dalam 4 tahun terakhir**, banyak terkait layanan digital dan pihak ketiga yang tidak menerapkan standar keamanan ketat.
- **Verizon DBIR 2024** menegaskan **68% breach melibatkan faktor manusia** (phishing, kesalahan konfigurasi, kelalaian vendor). Angka ini menyoroti pentingnya **kontrak keamanan vendor + kontrol teknis otomatis**.

4. Titik Kontrol Teknis (Controller ↔ Processor)

- **Untuk Pengendali:**
 - *Data Mapping*: pastikan semua aliran data ke vendor tercatat.
 - *Vendor Risk Rating*: pakai tools seperti **Cyber Rank** untuk menilai risiko pihak ketiga.
 - *SOAR Playbook*: otomatisasi respons insiden yang bersumber dari vendor.
- **Untuk Prosesor:**
 - *Zero Trust Access*: minimalisasi hak akses internal.
 - *Audit Log & Forensics*: siap diekspor ke SIEM pengendali.
 - *Dark Web Monitoring*: pantau kebocoran kredensial milik karyawan/vendor yang bisa jadi pintu masuk.

5. Implikasi UU PDP: Siapa Bertanggung Jawab?

- **Pengendali** tetap bertanggung jawab penuh di mata hukum, bahkan jika insiden bersumber dari vendor.
- **Prosesor** dapat terkena sanksi bila lalai menjaga keamanan atau melanggar instruksi pengendali.
- Sanksi administratif bisa mencapai **2% dari pendapatan tahunan**, dan untuk korporasi, denda bisa **10× lipat** dengan tambahan sanksi seperti pencabutan izin.

Ringkas untuk Engineer

- **Pengendali**: pikirkan *governance & oversight*.
- **Prosesor**: pikirkan *execution & evidence*.
- **Keduanya** harus mampu membuktikan kepatuhan lewat **policy-as-code, log terpusat, dan evidence pack**.

- **Supply-chain security** adalah area resiko terbesar: audit vendor bukan formalitas, tapi kewajiban strategis untuk bertahan di rezim UU PDP.

Tabel Perbandingan Peran Pengendali vs Prosesor Data (UU PDP)

Peran	Tugas Hukum	Kontrol Teknis (Contoh Implementasi)	Artefak Bukti Audit	SLA / KPI
Pengendali Data (Controller)	- Menentukan tujuan & cara pemrosesan data. - Menjamin <i>lawful basis</i> & prinsip minimisasi data. - Menyediakan hak subjek data (akses, koreksi, hapus, portabilitas). - Notifikasi insiden ≤ 3×24 jam. - Menunjuk DPO jika diperlukan.	- <i>Data Discovery & Mapping</i> (DSPM/DLP). - IAM & <i>purpose-based access</i>. - <i>Privacy Portal</i> untuk permintaan data subject. - SIEM + SOAR untuk deteksi & notifikasi insiden.	- Data inventory / <i>data flow map</i>. - Policy config (retensi, <i>lawful basis</i>). - SLA dashboard permintaan data subject. - Incident ticket & notice letter.	- SLA hak subjek ≤ 14 hari. - % permintaan selesai tepat waktu ≥ 95%. - SLA notifikasi insiden ≤ 72 jam. - Encrypted data coverage ≥ 95%.
Prosesor Data (Processor)	- Memproses data hanya sesuai instruksi pengendali. - Menyediakan jaminan teknis & organisasi (Pasal 39). - Membantu pengendali dalam hak subjek data. - Notifikasi insiden ke pengendali segera.	- <i>Logging & Monitoring</i> granular. - Zero Trust & least privilege access. - Audit log siap diekspor ke pengendali. - <i>Dark Web Monitoring</i> untuk kredensial internal.	- Config baseline. - Forensik log (akses, modifikasi, transfer). - SLA report untuk pengendali. - Bukti sertifikasi (ISO 27001, SOC 2).	- SLA eskalasi insiden ke pengendali ≤ 24 jam. - 100% akses user tercatat di log. - Review akses minimal 1×/kuartal. - False positive rate ≤ 5% pada log monitoring.

Intinya:

- **Pengendali** fokus pada *governance & oversight*: *lawful basis*, SLA ke regulator & data subject, serta *visibility end-to-end*.
- **Prosesor** fokus pada *execution & evidence*: kepatuhan kontraktual, keamanan teknis, dan kesiapan menyediakan log serta bukti audit.

Contoh DPA *Policy-as-Code* (YAML)

```
dpa:
  id: "dpa-controller-processor-2025"
  description: "Policy-as-code untuk mendefinisikan kewajiban Controller vs
Processor sesuai UU PDP"
  parties:
    controller: "BankXYZ Indonesia"
    processor: "CloudService ABC"
  obligations:
    controller:
      - ensure_lawful_basis: true
      - data_minimization: enforced
      - incident_notification: "≤ 72h to regulator & subjects"
      - dpo_designation: "mandatory if high-risk processing"
    processor:
      - process_only_on_instructions: true
      - technical_measures:
          - encryption: "AES-256 at rest, TLS 1.3 in transit"
          - access_control: "Zero Trust + MFA"
          - logging: "granular logs, 12 month retention"
      - incident_notification: "≤ 24h to controller"
      - assist_subject_rights: true
  evidence_pack:
    - config_baseline: required
    - audit_log_export: required
    - cert_iso27001: required
  kpi:
    controller:
      subject_request_sla_days: 14
      subject_request_on_time: "≥ 95%"
    processor:
      incident_escToolion_hours: 24
      access_review_frequency: "quarterly"
```

Contoh DPA *Policy-as-Code* (JSON)

```
{
  "dpa": {
    "id": "dpa-controller-processor-2025",
    "description": "Policy-as-code untuk kewajiban Controller dan Processor (UU PDP)",
    "parties": {
      "controller": "BankXYZ Indonesia",
      "processor": "CloudService ABC"
    },
    "obligations": {
      "controller": {
        "ensure_lawful_basis": true,
        "data_minimization": "enforced",
        "incident_notification": "≤72h",
        "dpo_designation": "mandatory_if_high_risk"
      },
      "processor": {
        "process_only_on_instructions": true,
        "technical_measures": {
          "encryption": "AES-256_rest_TLS1.3_transit",
          "access_control": "ZeroTrust_MFA",
          "logging": "granular_12m_retention"
        },
        "incident_notification": "≤24h_to_controller",
        "assist_subject_rights": true
      }
    },
    "evidence_pack": [
      "config_baseline",
      "audit_log_export",
      "iso27001_certificate"
    ],
    "kpi": {
      "controller": {
        "subject_request_sla_days": 14,
        "subject_request_on_time": "≥95%"
      },
      "processor": {
        "incident_escalation_hours": 24,
        "access_review_frequency": "quarterly"
      }
    }
  }
}
```

Catatan penting untuk engineer & auditor:

- YAML/JSON ini bisa dipakai sebagai **template kontraktual digital** antara Controller–Processor.
- Bisa di-*parse* ke dalam **GRC tools** atau di-*enforce* lewat *policy engine* (mis. OPA, HashiCorp Sentinel).
- Bagian **obligations & KPI** dapat langsung dipetakan ke **playbook SOAR** atau **compliance dashboard** untuk monitor real-time.

Kewajiban Keamanan & Pemberitahuan Insiden

Dalam kerangka **UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)**, aspek **keamanan pemrosesan data** dan **pemberitahuan insiden** menjadi titik krusial. Untuk engineer dan praktisi IT, ini bukan hanya soal *compliance*, tetapi juga *operational resilience* yang menentukan apakah organisasi mampu bertahan saat terjadi kebocoran data.

1. Kewajiban Keamanan (Security of Processing)

UU PDP Pasal 39(2) menegaskan bahwa **pengendali maupun prosesor wajib menerapkan langkah teknis dan organisasi untuk menjamin keamanan data pribadi**. Prinsip ini selaras dengan standar global seperti GDPR (Pasal 32).

Penerapan teknis yang wajib diperhatikan:

- **Enkripsi data *at rest* dan *in transit*.**
- **Identity & Access Management (IAM)** dengan prinsip *least privilege* dan **MFA**.
- **Data Loss Prevention (DLP) / Data Security Posture Management (DSPM)** untuk deteksi kebocoran data sensitif.
- **Security Information & Event Management (SIEM) + Endpoint Detection & Response (EDR)** untuk *real-time monitoring*.
- **Backup dengan immutability** agar tetap aman dari *ransomware*.

Statistik relevan:

- Menurut **Verizon DBIR 2024**, **68% insiden kebocoran data global melibatkan kesalahan manusia dan konfigurasi lemah**, menegaskan pentingnya *automated checks*.
- Di Indonesia, **94 juta data pribadi warga terekspos dalam 4 tahun terakhir**, banyak diantaranya akibat *misconfiguration* cloud dan lemahnya kontrol teknis.

2. Pemberitahuan Insiden (Breach Notification)

UU PDP Pasal 46 menetapkan standar ketat:

- **Pengendali wajib memberi tahu regulator & subjek data paling lambat 3×24 jam** sejak ditemukannya insiden kebocoran data.
- Notifikasi harus memuat **waktu insiden, jenis data yang terdampak, langkah mitigasi, dan kontak DPO**.
- **Prosesor** harus melaporkan insiden ke pengendali dalam waktu lebih singkat (praktik terbaik: ≤ 24 jam).

Implikasi untuk tim IT:

- Sistem deteksi harus otomatis memicu **alert + auto-notice generator** ke DPO dan manajemen risiko.
- Harus ada **template notice** siap pakai untuk regulator (*Kominfo*) dan untuk publik.
- Harus dipastikan **chain-of-custody log** tersedia sebagai bukti jika insiden diperiksa.

Statistik relevan:

- Laporan **IBM Cost of Data Breach 2023** menunjukkan rata-rata organisasi butuh **204 hari untuk mendeteksi insiden** dan **73 hari untuk mengendalikannya**, memperlihatkan *gap* serius dibanding SLA UU PDP (≤ 3 hari).
- Di ASEAN, rata-rata waktu pemberitahuan breach masih di atas **30 hari**, artinya Indonesia dengan UU PDP jauh lebih ketat dari praktik regional.

3. Konsekuensi Jika Gagal

Kegagalan memenuhi kewajiban keamanan & notifikasi insiden membawa konsekuensi serius:

- **Sanksi administratif:** teguran, penghentian kegiatan, denda hingga 2% pendapatan tahunan.
- **Sanksi pidana:** hingga 6 tahun penjara jika kelalaian menyebabkan kerugian besar.
- **Litigasi class action:** subjek data dapat menggugat kerugian.
- **Kerugian reputasi:** breach besar dapat menggerus kepercayaan publik secara permanen.

4. Rekomendasi Teknis untuk Engineer

- Implementasikan **policy-as-code** untuk enkripsi wajib, deteksi public link, dan notifikasi otomatis.
- Gunakan **SOAR playbooks** untuk mempercepat respons (contoh: auto revoke link, reset password, notify DPO).
- Monitor **KPI insiden**:
 - *Mean Time to Detect (MTTD)* < 48 jam.
 - *Mean Time to Respond (MTTR)* < 72 jam.
 - % insiden yang diberitahukan tepat waktu $\geq 99\%$.

Kesimpulan:

UU PDP menuntut organisasi tidak hanya *secure by design*, tetapi juga **resilient by default**. Untuk profesional IT, hal ini berarti membangun sistem yang mampu mendeteksi, merespons, dan membuktikan kepatuhan keamanan dalam waktu yang sangat singkat.

Template Notifikasi Insiden – Regulator

[Logo & Kop Surat Organisasi]

Nomor: [Nomor Surat]

Tanggal: [Tanggal Surat]

Kepada Yth,
Menteri Komunikasi dan Informatika Republik Indonesia
u.p. Direktur Jenderal Aplikasi Informatika
di Tempat

Perihal: Pemberitahuan Insiden Kebocoran Data Pribadi

Dengan hormat,

Sehubungan dengan kewajiban pemberitahuan insiden sesuai **Pasal 46 UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)**, bersama ini kami melaporkan terjadinya insiden kebocoran data sebagai berikut:

1. **Waktu Kejadian** : [Tanggal & Jam insiden terdeteksi]
2. **Jenis Data yang Terdampak** : [contoh: NIK, alamat email, nomor telepon, data kesehatan]
3. **Jumlah Subjek Data yang Terdampak** : [perkiraan jumlah individu]
4. **Penyebab Awal (Initial Cause)** : [mis. phishing, konfigurasi cloud, serangan malware]
5. **Langkah Mitigasi yang Dilakukan** :
 - Menonaktifkan akses publik / kredensial yang terekspos
 - Melakukan reset password pada akun terdampak
 - Mengaktifkan monitoring intensif pada sistem terkait
6. **Kontak Petugas Perlindungan Data Pribadi (DPO)** :
 - Nama: [Nama DPO]
 - Email: [alamat email DPO]
 - Telepon: [nomor kontak DPO]

Kami berkomitmen untuk menyampaikan laporan investigasi lanjutan (*incident report*) dalam waktu [x] hari kerja setelah investigasi forensik selesai.

Atas perhatian dan kerjasamanya, kami ucapkan terima kasih.

Hormat kami,
[TTD & Nama Pimpinan / DPO]
[Jabatan]

Template Notifikasi Insiden – Publik (Subjek Data)

Judul: Pemberitahuan Insiden Keamanan Data Pribadi

Yth. [Nama Pengguna / Pelanggan],

Kami dengan menyesal menginformasikan bahwa pada tanggal **[dd/mm/yyyy]**, telah terjadi insiden keamanan yang berpotensi mempengaruhi **data pribadi Anda**.

Rincian insiden:

- **Jenis Data yang Terdampak:** [mis. email, nomor telepon, NIK]
- **Waktu Insiden:** [dd/mm/yyyy, hh:mm]
- **Penyebab Awal:** [mis. akses tidak sah ke sistem database pelanggan]

Langkah yang sudah kami lakukan:

- Segera menutup akses yang tidak sah
- Melakukan reset kredensial dan peningkatan autentikasi (MFA)
- Melibatkan tim forensik untuk investigasi lanjutan
- Melaporkan insiden kepada regulator sesuai UU PDP

Langkah yang perlu Anda lakukan:

- Ganti password akun Anda segera
- Waspadai email, SMS, atau telepon mencurigakan (*phishing*)
- Hubungi pusat layanan kami jika menemukan aktivitas tidak wajar pada akun Anda

Kontak untuk pertanyaan lebih lanjut:

- Petugas PDP (DPO): [Nama & Kontak]
- Layanan Pelanggan: [nomor/email call center]

Kami memahami bahwa keamanan data Anda adalah prioritas utama. Kami mohon maaf atas ketidaknyamanan yang ditimbulkan dan berkomitmen untuk terus meningkatkan perlindungan data pribadi Anda.

Hormat kami,
[TTD & Nama Pimpinan / DPO]
[Jabatan]

Catatan Teknis untuk DPO & Tim IT:

- Template ini dapat dipadukan dengan **auto-notice generator (SOAR playbook)** agar memenuhi SLA **≤ 72 jam**.
- Disarankan melampirkan **FAQ** atau **portal khusus insiden** agar subjek data bisa memverifikasi status mereka.

Mapping UU PDP ↔ Kontrol Teknis

UU No. 27/2022 (UU PDP) membawa konsekuensi besar: setiap *pasal hukum* tidak boleh hanya berhenti di dokumen legal, tapi harus diturunkan menjadi **kontrol teknis yang terukur**. Bagi profesional IT, tantangan utamanya adalah membangun jembatan antara **bahasa hukum** dan **arsitektur teknologi**.

Tanpa pemetaan yang jelas, resiko terbesar adalah *compliance gap*—regulasi dipenuhi di atas kertas, tapi sistem IT gagal mencegah atau mendeteksi insiden nyata.

1. Data Minimization (Pasal 17–22)

- **Prinsip hukum:** Data pribadi hanya boleh diproses sesuai tujuan, relevan, dan tidak berlebihan.
- **Kontrol teknis:**
 - *Data Discovery & Classification* (DSPM, DLP) untuk menemukan dan menandai PII.
 - *Retention policy* otomatis untuk menghapus data yang sudah melewati masa simpan.
- **Bukti audit:** Laporan klasifikasi data, konfigurasi kebijakan retensi, log penghapusan otomatis.
- **KPI:** ≥90% data memiliki tag “purpose”; pelanggaran retensi ≤1%.

2. Lawful Basis & Consent (Pasal 20–23)

- **Prinsip hukum:** Setiap pemrosesan harus punya dasar hukum (persetujuan, kontrak, kewajiban hukum).
- **Kontrol teknis:**
 - *Consent Management Platform* (CMP).
 - IAM dengan *purpose-based access control*.
- **Bukti audit:** Database persetujuan, konfigurasi IAM, log akses berbasis tujuan.
- **KPI:** SLA response *consent withdrawal* ≤7 hari; akurasi pemetaan lawful basis ≥95%.

3. Security of Processing (Pasal 39)

- **Prinsip hukum:** Data harus dijaga kerahasiaan, integritas, dan ketersediaannya.
- **Kontrol teknis:**
 - Enkripsi *at rest & in transit* (AES-256, TLS 1.3).
 - IAM + MFA.
 - SIEM + EDR untuk deteksi real-time.
 - CASB untuk mengontrol SaaS.
- **Bukti audit:** Scan report, baseline config, laporan patching, tiket insiden.
- **KPI:** ≥95% data terenkripsi; patch SLA ≤7 hari; MFA coverage ≥98%.

4. Data Protection Impact Assessment (DPIA) (Pasal 34)

- **Prinsip hukum:** Proses berisiko tinggi wajib dianalisis sebelum dijalankan.

- **Kontrol teknis:**
 - Risk scoring engine.
 - Workflow DPIA dengan approval digital.
- **Bukti audit:** Dokumen DPIA, log persetujuan manajemen, register risiko.
- **KPI:** 100% proses berisiko tinggi memiliki DPIA; review ulang tahunan $\geq 1\times$.

5. Rights of Data Subject (Pasal 5–13)

- **Prinsip hukum:** Akses, koreksi, penghapusan, portabilitas, keberatan.
- **Kontrol teknis:**
 - *Self-service portal* untuk permintaan data.
 - API masking/anonymization.
- **Bukti audit:** Ticketing system, log response, data export log.
- **KPI:** SLA penyelesaian permintaan ≤ 14 hari; tingkat keberhasilan $\geq 95\%$.

6. Statistik Penting (2023–2024)

- **204 hari:** rata-rata waktu deteksi insiden global menurut IBM Cost of Data Breach 2023—jauh dari SLA notifikasi UU PDP (≤ 3 hari).
- **94 juta data bocor** di Indonesia dalam 4 tahun terakhir, banyak karena konfigurasi cloud yang salah.
- **35,5% breach global** melibatkan vendor pihak ketiga, menegaskan pentingnya pemetaan kontrol hingga rantai pasok.

7. Mengapa Mapping Penting?

- **Legal → Teknis:** Lawyer bicara pasal, engineer bicara enkripsi & SIEM. Mapping menjembatani keduanya.
- **Audit-ready:** Memudahkan penyusunan *evidence pack* (policy, scan, log, tiket).
- **Automasi:** Dengan *policy-as-code*, pemetaan bisa dipaksa lewat pipeline DevSecOps.

Kesimpulan untuk Engineer:

Setiap pasal dalam UU PDP harus diterjemahkan ke kontrol nyata: **DLP/DSPM untuk minimisasi, IAM untuk lawful basis, enkripsi & SIEM untuk security, workflow DPIA untuk high-risk, dan portal hak subjek untuk compliance**. Tanpa pemetaan ini, organisasi hanya compliant di kertas—bukan di lapangan.

BAB 3: Metodologi Audit & Skema Penilaian Tools

Tahap Audit

Audit privasi yang *berhasil* adalah yang **mengubah pasal hukum menjadi sinyal, kontrol, dan bukti**. Siklus 6 tahap di bawah ini dirancang agar **MTTD/MTTR** makin pendek, **eksposur PII** makin kecil, dan **bukti UU PDP** selalu siap. **Fakta lapangan:** biaya *data breach* global **US\$4,88 juta (2024)** dan turun ke **~US\$4,4 juta (2025)** saat identifikasi/containment makin cepat—indikasi kuat bahwa otomatisasi deteksi/respons memang *pay off*. ([IBM](#))

1. Discover — tahu di mana PII berada

Tujuan: inventarisasi *system of record*, *data store*, dan *data flow* termasuk SaaS & *shadow IT*.

Teknik & tooling:

- *DSPM/DLP* untuk *auto-discovery* PII (bucket S3/Blob, database, *collab drive*).
- Enrichment aset via *cloud inventory* + *SaaS connectors* (M365/Google, CRM, code repos).
- *Third-party mapping* (vendor/mitra) karena **supply chain** adalah sumber insiden yang terus naik.

Mengapa krusial: 68% **breach** masih melibatkan *human element*; salah *share* & *misconfig* sering baru ketahuan setelah bocor. **Banyak kebocoran terjadi karena data yang “tak terlihat”** di SaaS/endpoint. ([Verizon](#))

KPI: *coverage discovery* ≥ 90% aset kritikal; *unknown data stores* → **trend turun** tiap kuartal.

2. Classify — tahu apa yang sensitif

Tujuan: memberi label *purpose/retention/sensitivity* pada data sehingga kontrol bisa *policy-driven*.

Teknik & tooling:

- Klasifikasi PII (NIK/NPWP/medis/finansial) via *regex* + *ML detectors*; *data tagging* di *catalog*.
- *Purpose-based access* (IAM) untuk memisahkan *lawful basis*.

Mengapa krusial: tanpa klasifikasi, **minimisasi** & **retensi** tak bisa ditegakkan.

KPI: ≥ 90% objek data ber-tag *purpose*; *retention violations* ≤ 1%.

3. Protect — cegah eksposur sejak desain

Tujuan: menerapkan kontrol pencegahan: enkripsi, akses minimum, *hardening* konfigurasi.

Teknik & tooling:

- **Encryption at rest/in transit, IAM + MFA, EDR, CASB/SSPM, backup immutability.**
- **Policy-as-code** untuk menolak *public link* PII dan *over-sharing* di SaaS.
Fakta pendukung: DBIR 2024 menyorot *misconfig/cred abuse* sebagai jalur umum; *hardening + IAM + DLP/DSPM* adalah **kontrol inti security of processing**. ([Verizon](#))
KPI: MFA coverage ≥98%, encrypted data ≥95%, patch SLA ≤7 hari.

4. Detect — temukan lebih cepat dari penyerang

Tujuan: kurangi *dwell time* lewat korelasi sinyal & intel eksternal.

Teknik & tooling:

- **SIEM** untuk korelasi log; **UEBA** untuk anomali; **dark-web monitoring** (domain/email/brand) untuk *early warning* kredensial/artefak yang bocor.
- **Secrets scanning** (TruffleHog/Gitleaks) di CI/CD; **email/SaaS DLP** untuk *exfil*.
Fakta pendukung: SpyCloud 2025: **53,3 miliar identity records** “ter-recapture” (+22% YoY)—**volume kredensial/PII di underground** makin masif; deteksi eksternal **bukan opsional**. ([SpyCloud](#))
KPI: Mean Time to Detect (MTTD) < 48 jam; dark-web hit → reset ≤30 menit.

5. Respond — ubah *alert* jadi aksi otomatis

Tujuan: pembatasan dampak secepat mungkin sesuai *playbook* & UU PDP.

Teknik & tooling:

- **SOAR playbooks:** *revoke OAuth, force reset password, quarantine file, isolate endpoint, notify DPO*.
- **Breach runbook** khusus **UU PDP** untuk *draft notice* dan *contact list* regulator/subjek data.
Fakta pendukung: Studi & praktik industri menunjukkan **SOAR memangkas MTTR** secara nyata; Unit 42 & vendor-independen menekankan metrik **MTTD/MTTR** sebagai indikator kedewasaan SOC. ([Palo Alto Networks](#))
KPI: Mean Time to Respond (MTTR) < 72 jam; ≥60% insiden berulang auto-remediated.

6. Report — bukti siap audit & *learning loop*

Tujuan: menghasilkan paket bukti & ringkasan eksekutif untuk **regulator, DPO, dan manajemen**.

Teknik & tooling:

- **Evidence Pack otomatis:** *incident timeline, who/what/when, data types, remediation log, affected subjects estimate*, salinan **notice ≤3×24 jam**.
- **KPI dashboard** (MTTD/MTTR, coverage discovery/klasifikasi, *auto-remediation rate*, *vendor risk*).
Fakta pendukung: Riset IBM: **penurunan biaya ~9% (2025)** dikaitkan dengan **identifikasi & containment lebih cepat**—*reportability* bukan sekadar kepatuhan, melainkan *feedback loop* untuk efisiensi risiko. ([IBM](#))

KPI: SLA notifikasi UU PDP terpenuhi $\geq 99\%$; evidence pack siap ≤ 24 jam pasca-insiden.

Kenapa Siklus Ini Mendesak — *Reality Check*

- **Waktu deteksi historis masih lambat** (ratusan hari di banyak studi 2023/24) sehingga tak sejalan dengan **SLA UU PDP ≤ 72 jam**—*gap* ini hanya bisa ditutup dengan **korelasi SIEM + SOAR** dan **otomasi lintas SaaS/endpoint/cloud**. ([IBM](#))
- **Supply-chain/third-party** terus jadi pemicu insiden; tahap *Discover–Classify* harus mencakup **vendor/mitra** agar *Respond–Report* tidak *blind spot*. (Lihat DBIR 2024 perluasan definisi *third-party breach*). ([Verizon](#))
- **Kredensial & data di dark web** naik tajam (SpyCloud +22% YoY) → *Detect–Respond* wajib menutup loop: **intel** → **korelasi** → **reset/revoke otomatis**. ([SpyCloud](#))

Ops Guide singkat per tahap (siap dioperasikan)

- **Discover:** aktifkan konektor DSPM/DLP; *full crawl* objek cloud & shares; *asset register* tersinkron ke CMDB.
- **Classify:** *labeling PII + purpose*; *retention job* terjadwal; *policy exception review* mingguan.
- **Protect:** *encryption baseline*, **MFA $\geq 98\%$** , *SSPM policies* untuk *public link kill-switch*.
- **Detect:** *content DLP*, *secrets scanning*, **dark-web watchlist** domain/email/brand; *alert* → *SIEM*.
- **Respond:** **SOAR playbooks** (reset/revoke/quarantine/notify DPO); *table-top* triwulan.
- **Report:** *auto evidence pack + exec dashboard*; *post-incident review* dengan *action items* ter-track.

Ringkasnya

Discover–Classify–Protect–Detect–Respond–Report bukan slogan, tetapi **pabrik kontrol** yang menghubungkan UU PDP dengan realitas SOC: **lebih cepat menemukan, lebih cepat menutup, lebih mudah membuktikan**. Hasil akhirnya: **biaya insiden turun** dan **kepatuhan bisa diaudit kapan pun**. ([IBM](#))

Checklist Teknis per Tahap Audit

1. Discover

- **Konfigurasi Minimum**
 - DSPM/DLP diaktifkan dengan *connectors* ke cloud storage (S3, GDrive, OneDrive).
 - Agent endpoint aktif minimal di laptop staf yang mengakses PII.
- **Detectors**
 - *Regex* untuk NIK, NPWP, nomor kartu kredit, data medis dasar.

- ML-based classifier untuk dokumen legal/HR.
- **Playbooks**
 - *Scheduled crawl* tiap minggu → hasil ke CMDB + data catalog.
- **Artefak Bukti**
 - *Asset inventory* (CSV/JSON).
 - Laporan coverage discovery (% scanned vs total aset).

2. Classify

- **Konfigurasi Minimum**
 - *Data catalog* wajib punya field: *purpose*, *sensitivity*, *retention*.
- **Detectors**
 - Regex + ML untuk menandai “Sensitive” vs “Public” vs “Internal”.
- **Playbooks**
 - Auto-tagging saat data baru masuk repository.
- **Artefak Bukti**
 - Laporan % data dengan *purpose tag*.
 - Exception report untuk data tanpa label.

3. Protect

- **Konfigurasi Minimum**
 - **Encryption at rest & transit.**
 - MFA coverage ≥ 98%.
 - SaaS Security Posture Management (SSPM) untuk *public link blocking*.
- **Detectors**
 - Misconfig rules: *public bucket*, *open share*, *no encryption*.
- **Playbooks**
 - Kill public link (lihat YAML di bawah).
 - Quarantine file yang *policy-violating*.
- **Artefak Bukti**
 - Log perubahan permission.
 - Screenshot *encryption settings*.
 - Policy report (SSPM/DLP).

4. Detect

- **Konfigurasi Minimum**

- SIEM (misal: Wazuh, ELK, Splunk) ingest log SaaS, endpoint, firewall.
- **Detectors**
 - *Secrets scanning* di Git/CI (TruffleHog/Gitleaks).
 - Dark-web monitoring domain/email.
- **Playbooks**
 - Alert → auto reset password bila domain/email muncul di *dark web*.
 - Quarantine endpoint saat IOC muncul.
- **Artefak Bukti**
 - SIEM alert log.
 - Intel feed screenshot.
 - Incident ticket dengan timestamp.

5. Respond

- **Konfigurasi Minimum**
 - SOAR terhubung ke IAM, M365/Google, endpoint security.
- **Detectors**
 - IOC feed → SOAR trigger.
 - SaaS DLP trigger.
- **Playbooks**
 - Auto revoke OAuth token mencurigakan.
 - Force reset password user terdampak.
 - Notify DPO via email + ticket.
- **Artefak Bukti**
 - Timeline insiden.
 - *Remediation log*.
 - *Notification letter* (draft auto-generated).

6. Report

- **Konfigurasi Minimum**
 - Dashboard eksekutif: MTDD, MTTR, coverage discovery, % auto-remediation.
- **Detectors**
 - SLA breach (notifikasi terlambat > 72 jam).
- **Playbooks**
 - Auto-generate incident summary → PDF/JSON.
 - Compile evidence pack untuk regulator.
- **Artefak Bukti**

- PDF “Evidence Pack”.
- Email log ke regulator.
- SLA compliance dashboard.

Contoh *Policy-as-Code*

A. Public-Link Kill-Switch (SaaS/Cloud Drive)

Format YAML — bisa dipakai di **Open Policy Agent (OPA)** atau **SOAR rule engine**

```
policy:
  id: public_link_killswitch
  description: "Blokir semua link publik untuk file dengan tag PII"
  trigger:
    - event: file_share_created
  condition:
    all:
      - field: file.tag
        in: ["PII", "Sensitive"]
      - field: share.visibility
        equals: "public"
  action:
    - type: revoke_share
    - type: notify
      channel: "dpo-alerts"
      message: "Public link on PII file revoked automatically"
    - type: log
      target: "audit/evidence_pack.log"
```

B. Auto-Notice Generator (UU PDP – ke Regulator & Publik)

Format JSON — *policy-as-code* untuk SOAR/incident automation

```
{
  "policy_id": "auto_notice_generator",
  "description": "Generate PDP Incident Notice within SLA",
  "trigger": {
    "event": "incident_confirmed",
    "severity": "high",
    "data_tags": ["PII", "Sensitive"]
  },
  "actions": [
    {
      "type": "template_fill",
      "template": "incident_notice_v1",
      "fields": {
        "organization": "ACME Corp",
        "incident_id": "{{incident.id}}",
        "data_subjects": "{{incident.affected_count}}",
        "breach_date": "{{incident.start_time}}",
        "detection_date": "{{incident.detect_time}}",
        "containment_date": "{{incident.close_time}}",

```

```

        "remediation": "{{incident.remediation_summary}}"
    }
},
{
    "type": "send_email",
    "recipients": ["regulator@pdp.go.id", "public_notice@company.com"],
    "subject": "Mandatory PDP Breach Notice",
    "body_from_template": "incident_notice_v1"
},
{
    "type": "archive",
    "target": "audit/incident_notices/{{incident.id}}.json"
}
]
}

```

Dengan **checklist ini + *policy-as-code***, tim IT langsung punya *baseline* audit & *automation blueprint* untuk UU PDP:

- Ada *guardrails* (kill-switch link publik),
- Ada *notification engine* (auto notice ke regulator/public),
- Ada artefak bukti siap audit (logs, evidence pack, SLA metrics).

Kriteria Evaluasi (Skor 1–5)

Dalam praktik profesional, pemilihan tool untuk audit privasi tidak bisa berdasarkan klaim vendor semata. Harus ada **rubrik evaluasi objektif** yang menilai aspek teknis, kepatuhan, otomasi, dan biaya secara terukur. Model skoring **1–5** memungkinkan konsistensi lintas proyek dan memudahkan perbandingan antar *tools*.

1. Automated Privacy Audit

- **Definisi:** Kemampuan tool melakukan *scheduled scan* otomatis dengan cakupan luas (database, file server, SaaS, endpoint).
- **Indikator:**
 - Skor 1: Scan manual, terbatas ke 1–2 sumber.
 - Skor 3: Ada jadwal otomatis, cakupan terbatas (cloud storage populer).
 - Skor 5: Multi-connector (on-prem, cloud, SaaS), dengan dashboard SLA.
- **Statistik relevan:** IBM 2023 mencatat **82% organisasi global** sudah mengadopsi otomasi parsial dalam audit keamanan, tapi di Indonesia adopsi DSPM/DLP masih <20%.

2. Data Leak Detection (SaaS/Email/Repo/File Share)

- **Definisi:** Kemampuan mendeteksi *data at risk* yang bocor via email, repositori Git, atau file share publik.
- **Indikator:**
 - Skor 1: Hanya mengandalkan laporan insiden manual.
 - Skor 3: Ada plugin email/repo scanner.
 - Skor 5: Integrasi penuh dengan SaaS (O365, GDrive, GitHub) + *real-time alerts*.
- **Statistik relevan:** **45% kebocoran data** di Asia Tenggara 2023 bersumber dari *misconfigured SaaS*.

3. Password Leak Check

- **Definisi:** Cross-check password dengan database breach (HIBP, SpyCloud) + enforcement policy.
- **Indikator:**
 - Skor 1: Tidak ada pengecekan breach.
 - Skor 3: Manual lookup (HIBP API).
 - Skor 5: Integrasi IAM, auto reset password jika ditemukan bocor.
- **Statistik relevan:** **80% breach global** masih melibatkan kredensial lemah atau bocor.

4. Sensitive-Info Leak (Regex/ML)

- **Definisi:** Deteksi kebocoran NIK, NPWP, CC, data medis via regex/ML.
- **Indikator:**
 - Skor 1: Regex manual tanpa otomasi.
 - Skor 3: Regex bawaan vendor.
 - Skor 5: Kombinasi regex + ML + masking otomatis.
- **Statistik relevan:** Di Indonesia, kebocoran **94 juta data pribadi** dalam 4 tahun terakhir sebagian besar melibatkan NIK dan data kesehatan.

5. Dark Web Monitoring

- **Definisi:** Pemantauan forum, marketplace, chat underground terkait domain/email organisasi.
- **Indikator:**
 - Skor 1: Manual search via OSINT.
 - Skor 3: Ada intel feed tapi tidak otomatis.
 - Skor 5: Realtime monitoring + integrasi SIEM/SOAR.
- **Statistik relevan:** **35,5% breach global** berasal dari vendor pihak ketiga, banyak terdeteksi pertama kali di forum underground.

6. Automatic Advice & Remediation (SOAR/Playbooks)

- **Definisi:** Kemampuan tool memberi rekomendasi teknis dan mengeksekusi tindakan otomatis (reset password, blokir link, quarantine file).
- **Indikator:**
 - Skor 1: Rekomendasi manual saja.
 - Skor 3: Ada template playbook.
 - Skor 5: Integrasi penuh ke SOAR dengan auto-remediation.
- **Statistik relevan:** Perusahaan dengan *AI-driven SOAR* mampu memangkas biaya insiden rata-rata **USD 1,76 juta** dibanding tanpa otomasi.

7. Compliance & Reporting (UU PDP/ISO/GDPR)

- **Definisi:** Kemampuan menghasilkan laporan siap audit sesuai regulasi.
- **Indikator:**
 - Skor 1: Tidak ada template.
 - Skor 3: Template GDPR/ISO.
 - Skor 5: Customizable ke UU PDP + auto evidence pack.
- **Nilai tambah:** Indonesia akan menegakkan penuh UU PDP mulai **Oktober 2024**, denda administratif maksimal **2% omzet tahunan**.

8. Integrasi & Operasional (SIEM, Ticketing, False Positive Mgmt)

- **Definisi:** Kemampuan integrasi dengan stack SOC & workflow existing.
- **Indikator:**
 - Skor 1: Tidak ada integrasi.
 - Skor 3: Integrasi SIEM saja.
 - Skor 5: SIEM + ticketing + API + *false positive tuning*.

9. Biaya & TCO (Total Cost of Ownership)

- **Definisi:** Evaluasi lisensi, infrastruktur, SDM, serta rata-rata MTTR.
- **Indikator:**
 - Skor 1: Lisensi mahal, perlu infra besar, tim khusus.
 - Skor 3: SaaS dengan biaya menengah.
 - Skor 5: OSS/low-cost + integrasi mudah.
- **Statistik relevan:** Rata-rata biaya kebocoran data di Indonesia **USD 2,16 juta** per insiden (IBM 2023), lebih rendah dari global (USD 4,45 juta) tapi meningkat 8% YoY.

Kesimpulan untuk engineer:

- Pastikan tools bukan hanya compliant, tapi **detektif aktif** (detect + auto-respond).
- Jangan terjebak vendor lock-in — evaluasi harus berbasis metrik dan *evidence pack*.
- Skor 1–5 membuat setiap pilihan dapat dipertanggungjawabkan ke manajemen dan regulator.

Tabel Rubrik Skoring Audit Data Privacy (UU PDP)

Kriteria	Skor 1 (Low / Immature)	Skor 3 (Medium / Partially Mature)	Skor 5 (High / Mature)	Bukti Audit
Automated Privacy Audit	Scan manual, terbatas ke 1–2 sistem (file server/DB).	Ada <i>scheduled scan</i> , terbatas ke cloud storage populer.	Multi-connector (on-prem, SaaS, DB, endpoint) + dashboard SLA.	Log jadwal scan, screenshot dashboard, report hasil scan.
Data Leak Detection (SaaS/Email/Repo)	Hanya bergantung laporan manual insiden.	Deteksi via plugin email/repo scanner terbatas.	Integrasi penuh (O365, GDrive, GitHub, file share) + real-time alert.	Log alert SIEM, tiket insiden, sample laporan exposure.
Password Leak Check	Tidak ada pengecekan breach.	Manual lookup (HIBP API / SpyCloud CSV).	Terintegrasi IAM, auto reset password bila bocor.	Log IAM reset, feed HIBP/SpyCloud, bukti policy enforcement.
Sensitive Info Leak (NIK, NPWP, CC, Medis)	Regex manual terbatas.	Regex bawaan vendor untuk PII umum.	Regex + ML + masking otomatis.	Regex/ML config, hasil scan PII, log masking.
Dark Web Monitoring	Manual OSINT (Ahmia, forum publik).	Intel feed tersedia tapi tidak real-time.	Monitoring domain/email secara real-time, integrasi SIEM/SOAR.	Intel report, IOC feed, tiket korelasi insiden.

Automatic Advice & Remediation (SOAR)	Rekomendasi manual tanpa otomasi.	Ada template playbook (manual trigger).	Auto-remediation (kill switch, revoke token, reset password).	Playbook YAML/JSON, log eksekusi SOAR, remediation tracker.
Compliance & Reporting (UU PDP/ISO/GDPR)	Tidak ada template laporan kepatuhan.	Template GDPR/ISO tersedia.	Laporan siap audit sesuai UU PDP, evidence pack otomatis.	PDF report, mapping UU PDP ↔ kontrol teknis, evidence pack.
Integrasi & Operasional (SIEM, Ticketing)	Tidak ada integrasi.	Integrasi SIEM terbatas, tanpa tiket.	Full integrasi (SIEM, tiket, API, false positive mgmt).	Log SIEM, tiket insiden, bukti tuning false positive.
Biaya & TCO	Lisensi mahal, butuh infra besar + tim khusus.	SaaS mid-tier, biaya predictable.	OSS/low-cost + mudah integrasi.	Proposal biaya, TCO sheet, SLA tim ops.

Catatan penggunaan:

- Skor 1 → tool minim fungsi, hanya *checkbox compliance*.
- Skor 3 → ada otomasi parsial, tapi masih silo.
- Skor 5 → tool end-to-end, evidence siap regulator, terintegrasi SOC.
- Kolom *Bukti Audit* wajib diisi setiap assessment untuk menghindari bias opini.

Bobot Rekomendasi

Dalam praktik audit privasi, memilih tool tidak bisa sekadar berdasarkan harga atau popularitas vendor. Perusahaan di Indonesia harus menyeimbangkan **ketahanan teknis, kepatuhan hukum, kapasitas otomasi, dan total biaya operasional (TCO)**. Karena itu, digunakan bobot evaluasi berikut: **Teknis 40% | Kepatuhan 25% | Otomasi 20% | TCO 15%**.

1. Dimensi Teknis (40%)

Aspek teknis mendominasi bobot evaluasi karena **serangan siber semakin kompleks**.

- Indonesia masuk **10 besar negara dengan jumlah akun terbocor terbesar di dunia**, dengan lebih dari **16 juta data kredensial bocor sepanjang 2023** (sumber: Surfshark Breach Report 2023).
- Fitur inti yang diuji: *data discovery, classification, sensitive info detection* (NIK, NPWP, CC, rekam medis), *dark web monitoring*, dan *remediation* melalui SIEM/SOAR.
- Tool yang hanya menyajikan *compliance reporting* tanpa *threat detection* akan langsung jatuh skornya.

Contoh kontrol teknis:

- DSPM (BigID, Securiti) → auto-discovery PII di multi-cloud.
- Wazuh + custom rules → deteksi kebocoran data via log SIEM.
- DarkRadar.io → deteksi kredensial di *underground market*.

2. Dimensi Kepatuhan (25%)

UU No. 27/2022 (UU PDP) mulai berlaku penuh **Oktober 2024**. Risiko hukum sangat signifikan:

- **Sanksi administratif** hingga **2% dari pendapatan tahunan**.
- **Pidana penjara** (2–6 tahun) dan **denda miliaran rupiah** untuk pelanggaran serius.
- Kewajiban **notifikasi insiden maksimal 72 jam** ke regulator dan subjek data.

Karena itu, 25% bobot difokuskan pada:

- Apakah tool menyediakan template laporan sesuai format **UU PDP + ISO 27001 + GDPR**?
- Apakah ada fitur *evidence pack generator* untuk audit eksternal?
- Apakah ada *mapping PDP ↔ kontrol teknis* sehingga engineer tahu harus menyiapkan bukti apa?

3. Dimensi Otomasi (20%)

Dalam konteks SOC modern, **kecepatan respons lebih kritis daripada deteksi**.

- Data IBM Cost of a Data Breach 2023: **rata-rata breach diidentifikasi dalam 277 hari**; perusahaan dengan otomasi & AI menurunkan waktu deteksi hingga **108 hari lebih cepat**.
- Otomasi mengurangi **Mean Time To Detect (MTTD)** dan **Mean Time To Respond (MTTR)**.
- Fitur yang masuk penilaian:
 - *SOAR playbooks* untuk reset password otomatis.
 - *Kill switch* publik link di cloud storage (M365, GDrive).
 - *Auto-notice generator* untuk DPO agar siap mengirim notifikasi regulator.

4. Dimensi TCO (15%)

Biaya tetap penting, meski porsi lebih kecil (15%) karena keamanan dan kepatuhan harus tetap prioritas.

- Banyak organisasi di Indonesia (terutama Pemda dan RS pendidikan) masih **budget-sensitive**.
- **Open-source stack (Wazuh, Suricata, TruffleHog)** bisa menghemat hingga **70% dari biaya lisensi vendor komersial**, namun butuh tim yang kompeten untuk konfigurasi.
- Skor TCO mempertimbangkan:
 - Harga lisensi & subscription.
 - Biaya infra (cloud/on-prem).
 - Resource SDM (jumlah FTE yang dibutuhkan untuk operasional).

Kesimpulan Praktis

- **Teknis (40%)** memastikan tool benar-benar bisa **mencegah dan mendeteksi kebocoran data**.
- **Kepatuhan (25%)** adalah jembatan antara engineer ↔ regulator, wajib karena UU PDP membawa konsekuensi hukum berat.
- **Otomasi (20%)** menurunkan risiko human error dan mempercepat respon insiden.
- **TCO (15%)** membantu manajemen menyeimbangkan **biaya vs value**.

Dengan model bobot ini, CIO/DPO bisa melakukan **multi-criteria decision-making (MCDM)** yang obyektif, sehingga rekomendasi final bukan sekadar subjektif, tapi berbasis **skoring, bukti audit, dan konteks risiko lokal Indonesia**.

BAB 4: Pemetaan Kontrol: Dari UU PDP ke Fitur Tool

Matriks Pasal/Prinsip ↔ Kontrol ↔ Artefak Bukti

Bagi engineer, **pasal hukum** baru bernilai jika bisa diterjemahkan menjadi **kontrol teknis yang terukur** dan **bukti audit** yang konsisten. Di tengah biaya *data breach* global yang naik ke **US\$4,88 juta (2024)** dan tren eksposur identitas di *dark web* yang tumbuh **+22% YoY** (53,3 miliar *records* “ter-recapture”, 2025), kemampuan menghubungkan **UU PDP → kontrol → artefak** bukan opsional—ini *operational must*. ([IBM](#))

Matriks Pasal/Prinsip ↔ Kontrol ↔ Artefak Bukti

Catatan: istilah *tools* contoh: **DSPM/DLP** (BigID/Securiti/Purview), **CASB/SSPM, IAM/MFA, EDR/SIEM/UEBA, SOAR**.
Sumber pasal rujukan: **UU No. 27/2022**—lihat khususnya **Pasal 38–39** (keamanan pemrosesan), **Pasal 34 (DPIA)**, **Pasal 5–13 (hak subjek)**, **Pasal 20–23 (dasar pemrosesan)**, **Pasal 46 (notifikasi insiden)**. ([JDIH Kemkomdigi](#))

Pasal / Prinsip UU PDP	Kontrol Teknis (contoh implementasi)	Artefak Bukti (audit-ready)	KPI/Target
Security of Processing (Pasal 38–39)	Enkripsi <i>at rest/in transit</i> ; IAM + MFA ; EDR di endpoint; CASB/SSPM cegah <i>misconfig</i> SaaS; DLP/DSPM cegah <i>exfiltration</i> .	<i>Crypto config baseline</i> , daftar <i>KMS keys</i> , laporan patching, <i>EDR policy export</i> , <i>CASB misconfig report</i> , tiket insiden.	Encrypted data ≥95% , MFA coverage ≥98% , <i>patch SLA ≤7 hari</i> . (JDIH Kemkomdigi)
Data Minimization & Retention (Pasal 17–22)	DSPM auto-discovery + tagging purpose , <i>retention policy</i> otomatis, <i>tokenization/masking</i> .	<i>Data catalog</i> (tag purpose/retention), log penghapusan otomatis, <i>retention exception list</i> .	≥90% objek data ber-tag purpose , <i>retention violation ≤1%</i> .

Lawful Basis & Consent (Pasal 20–23)	<i>Consent Management Platform; IAM dengan purpose-based access control; attribute-based policy di gateway/API.</i>	Database persetujuan, <i>access policy</i> per tujuan, log akses berbasis <i>purpose</i> .	Akurasi pemetaan dasar hukum ≥95% ; SLA <i>withdrawal</i> ≤7 hari .
Rights of Data Subject (Pasal 5–13)	<i>Self-service portal</i> hak subjek; <i>data export tooling</i> ; <i>erasure workflow</i> ; <i>field-level audit</i> .	Tiket <i>request</i> (akses/koreksi/hapus/portabilitas), log <i>fulfillment</i> , <i>export manifest</i> .	Penyelesaian permintaan ≤14 hari pada ≥95% kasus.
DPIA – High Risk (Pasal 34)	<i>Risk scoring engine</i> ; <i>DPIA workflow</i> dengan <i>digital approval</i> ; <i>change gating</i> di CI/CD untuk proses berisiko.	Dokumen DPIA, log persetujuan (CPO/CISO/DPO), <i>risk register + mitigation plan</i> .	100% proses berisiko tinggi punya DPIA; <i>review tahunan</i> ≥1× .
Breach Notification (Pasal 46)	SIEM/UEBA untuk deteksi; SOAR playbooks (reset password, revoke token, <i>public link kill-switch</i> , <i>notice generator</i>); dark-web monitoring untuk <i>early warning</i> .	<i>Incident timeline</i> , <i>SOAR run log</i> , <i>notice letter</i> (regulator & publik), <i>affected subjects estimate</i> .	SLA notifikasi ≤72 jam terpenuhi ≥99% ; MTTD <48 jam , MTTR <72 jam . (JDIH Kemkomdigi)
Third-Party / Processor Governance (lintas pasal kewajiban pengendali & prosesor)	<i>Vendor risk scoring</i> (contoh: Cyber Rank); <i>DPA policy-as-code</i> ; <i>ingest security attestations</i> (ISO/SOC2); pemantauan <i>dark web</i> kredensial vendor.	<i>DPA JSON/YAML</i> , hasil <i>third-party scan</i> , bukti kontrol prosesor (<i>shared responsibility matrix</i>), tiket <i>remediation</i> .	100% vendor kritikal punya DPA + penilaian tahunan; <i>closure temuan</i> ≤30 hari .

Konteks ancaman: *Human element* masih mendominasi – **68% breach** melibatkan faktor manusia (phishing/misconfig/credential abuse). Artinya kontrol di atas harus **mengatasi kesalahan manusia dan supply chain**—tidak cukup *checkbox compliance*. ([Verizon](#))

Contoh “Security of Processing” → kontrol → bukti (diperluas)

- **DLP/DSPM:** *auto-discovery* PII di *cloud buckets, file shares, DB*; *policy* blok *public link* untuk berkas bertag **Sensitive/PII**.
 - **Bukti:** *discovery coverage report, policy export, scan result CSV, exception register*.
- **CASB/SSPM:** cegah *misconfiguration* (contoh: *Anyone with link* di M365/GDrive).
 - **Bukti:** *misconfig baselines, remediation log, change ticket*.
- **EDR + SIEM:** deteksi *exfil* via *watchlist* dan *content rules*; korelasi *UEBA*.
 - **Bukti:** *alert artifacts, correlation graph, triage notes*.
- **SOAR:** *auto-remediate* (revoke token, *kill-switch*, reset), **generate notice** untuk DPO.
 - **Bukti:** *SOAR runbook log, evidence pack, notice sent log*.

Mengapa ini penting: Ketika *identity data* bocor di *dark web* meledak ke **53,3 miliar records** (2025), *prevention* saja tidak cukup; dibutuhkan **deteksi + respons otomatis** agar *blast radius* minimal dan **SLA notifikasi ≤72 jam** terpenuhi. ([SpyCloud](#))

Format artefak bukti (*audit-ready checklist*)

- **Policy dump** (YAML/JSON): enkripsi, *access control, retention*.
- **Scan reports:** *discovery/classification, DLP hits, misconfig*.
- **Logs:** SIEM (*alerts, correlation, enrichment*), **SOAR run logs** (aksi otomatis).
- **Tickets:** *incident, change, exception*.
- **Notices:** draf surat regulator & publik (+ *timestamp* pengiriman).
- **Metrik:** **MTTD/MTTR**, *coverage, exception aging, SLA notifikasi*.

Tabel Pemetaan UU PDP → Kontrol Teknis → Artefak Bukti → KPI

Pasal Kunci (UU PDP)	Kontrol Teknis	Artefak Bukti Audit	KPI (Key Performance Indicator)
Pasal 5–13: Hak Subjek Data (akses, perbaikan, penghapusan, keberatan, portabilitas)	- <i>Subject Rights Portal</i> (self-service) - Data catalog & search - Redaction/masking API	- Ticketing log - SLA dashboard - Data export log	- SLA penyelesaian permintaan ≤ 14 hari - % permintaan selesai tepat waktu ≥ 95%
Pasal 17–22: Prinsip & Dasar Hukum (lawful basis, minimization)	- Data classification & minimization engine (DSPM/DLP) - IAM <i>purpose-based access</i> - Retention scheduler	- Data inventory - Policy config snapshot - Access log	- % data bertag “purpose” ≥ 90% - Retention violation ≤ 1%
Pasal 34: DPIA (<i>high-risk processing</i>)	- Risk scoring engine - DPIA workflow & approval - Mitigation register	- DPIA report (PDF) - Approval trail - Residual risk acceptance	- Semua <i>high-risk process</i> punya DPIA 100% - Review ulang tahunan 100%
Pasal 39(2): Keamanan Pemrosesan	- Encryption at rest/in transit - IAM/MFA/SSO - EDR/AV - SIEM/DLP/DSPM - Backup immutability	- Scan report - Config baseline - Alert log - Pentest report	- Encrypted data ≥ 95% - MFA coverage ≥ 98% - Patch SLA ≤ 7 hari
Pasal 46: Notifikasi Insiden ≤ 3×24 jam	- Breach detection (SIEM/SOAR) - Auto notice generator - Incident response playbook	- Incident timeline - Notice letter copy - List subjek terdampak	- SLA notifikasi regulator/subjek ≤ 72 jam - % notifikasi tepat waktu ≥ 99%

Pasal 53: Penunjukan Petugas PDP (DPO)	- Compliance dashboard - DPO reporting workflow	- Laporan DPO - Risk/compliance dashboard	- Meeting compliance rutin ≥ 1×/bulan - SLA eskalasi insiden ≤ 24 jam
Pasal 56: Transfer Data ke Luar Negeri	- Geo-fencing policy - Transfer risk assessment - Contractual safeguards (SCC-like)	- Transfer assessment - Vendor contract - Legal memo	- 100% transfer lintas negara punya risk assessment - SLA approval ≤ 14 hari
Pasal 57–70: Sanksi & Penegakan	- Policy-as-code (deny misconfig) - Audit log centralization - SOAR playbook evidence pack	- Config deny logs - Evidence pack (zip) - Incident ticketing log	- Bukti audit lengkap ≤ 24 jam - False positive ≤ 5%

Contoh *YAML Policy-as-Code*

1. Public Link Kill-Switch (M365/GDrive/SharePoint)

(mencegah & auto-revoke link publik yang berisi PII/Confidential)

```

policy:
  id: public-link-kill
  description: "Auto revoke public links with sensitive data exposure"
  trigger:
    - event: "file.shared_public"
    - condition:
        - data.scan.contains_pii true
  action:
    - type: "revoke_public_link"
    - type: "notify"
      target: "DPO@company.id"
      message: "Public link revoked: {{file.name}} (owner:
{{user.id}})"
    - type: "log"
      destination: "SIEM"
  fields:
    - file.name
    - file.owner
    - timestamp

```

2. Auto-Notice Generator (Breach Detection → Notifikasi 3×24 jam)

(otomatis membuat draft notice untuk regulator & subjek data terdampak)

policy:

id: breach-auto-notice

description: "Generate breach notification within 72h SLA"

trigger:

- event: "incident.confirmed"
- condition:
 - incident.impact.data_subjects >= 1

action:

- type: "generate_notice"
 - template: "breach_notice_v1"

fields:

- incident.id
- incident.time
- incident.data_types
- mitigation_steps
- type: "dispatch_email"
 - recipients:
 - "regulator@kominform.go.id"
 - "affected_users_list.csv"

- type: "log"
 - destination: "SIEM"

fields:

- incident.id
- notice.id
- dispatch.status

Intinya:

- Tabel memberi **pasal** → **kontrol** → **bukti** → **KPI** yang siap dipakai auditor.
- YAML contoh memperlihatkan bahwa *policy-as-code* bisa langsung menegakkan pasal: *kill public link PII* (Pasal 39 & 57) dan *notifikasi ≤ 72 jam* (Pasal 46).
- **Template Evidence Pack** untuk audit (ceklist + sampel log).

Ringkasan eksekutif (untuk manajemen)

- **Matriks Pasal → Kontrol → Bukti** memastikan **UU PDP** tidak berhenti di dokumen, tetapi **mengunci konfigurasi teknis dan bukti**.
- Dengan **SIEM + SOAR + DSPM/DLP + CASB/SSPM**, organisasi menutup celah **misconfig, credential abuse, dan supply-chain leak**—akar dari mayoritas insiden (human element ~68%). ([Verizon](#))
- Hasilnya: **biaya insiden** lebih rendah (tren IBM 2024/2025), **notifikasi on-time**, dan **evidence pack** siap kapan pun diminta regulator. ([IBM](#))

BAB 5: Cyber Rank untuk Audit Data Privacy & Vendor Risk Management

Audit privasi data kini tidak hanya fokus pada sistem internal, tetapi juga **risiko eksternal** dari vendor dan mitra bisnis. **Survei Deloitte (2023)** menunjukkan 74% organisasi percaya reputasi mereka bisa rusak cepat akibat *cyber incident* di media sosial/vendor, sementara hanya 27% yang sadar akan konsekuensi etis.

Cyber Rank hadir dengan **skor risiko eksternal** berbasis AI yang menilai:

- *Privacy testing* seperti evaluasi cookie/consent banner.
- Penilaian kepatuhan regulasi lokal (UU PDP, DORA, BSSN).
- **Monitoring real-time** terhadap *attack surface* vendor tanpa intrusif.

Menurut Cyber Rank, biaya rata-rata tahunan untuk *continuous vendor monitoring* adalah **USD/vendor** — jauh lebih rendah dibanding pemain global seperti BitSight/Scorecard (**USD 1.500–2.000/vendor**).

Kasus Penggunaan

1. Due Diligence Vendor (pra-kontrak)

Tujuan: mencegah *blind spot* sebelum kontrak dan memastikan vendor laik PDP.

Apa yang dilakukan Cyber Rank

- **Verifikasi keamanan eksternal non-intrusif** (*attack surface*, ekspos layanan, kerentanan publik, *breached credentials*), plus **privacy testing** (kebijakan, cookie/consent) untuk menilai *privacy posture* awal. **Output: Skor risiko vendor** untuk *go/no-go decision* dan *tiering* (critical/high/standard).
- **Legal security clause detection** pada draf/perjanjian: *breach notification*, *data residency/sovereignty*, standar kontrol (mis. **ISO 27001/SOC 2**), hak audit, pengungkapan *sub-processor*. **Output: Clause map** (*pass/fail*) yang langsung bisa jadi lampiran kontrak.
- **Upload & verifikasi sertifikasi** oleh vendor (ISO/SOC2/penilaian internal). Sistem memvalidasi dan **menyesuaikan skor** berbasis bukti—mengurangi bias *self-attest*. **Output: Certificate verification log**.

Kenapa krusial (data-driven)

- **Third-party attack naik signifikan.** FT melaporkan **30% dari 7.965 serangan 2024** berasal dari pihak ketiga—**2×** tahun sebelumnya. **Makna:** *weak link* vendor jadi jalur favorit penyerang. ([Financial Times](#))
- **Biaya kebocoran data terus tinggi.** Rata-rata global 2024 **USD 4,88 juta** (naik dari USD 4,45 juta); industri finansial **~USD 6,08 juta**. **Implikasi:** tanpa *due diligence* dan otomasi, **MTTR** membengkak. ([IBM](#))

- **Regulasi: UU PDP (No. 27/2022)** menegaskan **Pengendali Data tetap bertanggung jawab** walau insiden terjadi di vendor—*due diligence* bukan sekadar *best practice*, tapi **kewajiban**. ([Hukumonline Learning](#))

Efisiensi biaya

- Pemantauan kontinu oleh Cyber Rank ± **USD/vendor/tahun** dengan **unlimited users**; bandingkan pemain global jauh lebih mahal **USD 1.500–2.000/vendor**.
Dampak: *coverage* luas untuk ratusan/ribuan vendor tanpa *seat cap*.

Artefak bukti (siap audit PDP)

- **Vendor Risk Scorecard** (tren & benchmark), **Privacy Findings** (cookie/consent), **Contract Clause Map**, **Certificate Log**, + **recommendation**.

2. Pemantauan Berkala Third-Party (pasca-onboarding)

Tujuan: mempertahankan *risk posture* vendor selama masa kontrak dan memenuhi kewajiban pengawasan berkelanjutan UU PDP.

Apa yang dilakukan Cyber Rank

- **Monitoring real-time skala besar:** mampu memantau ribuan vendor secara non-intrusif; organisasi bisa memilih *real-time* atau *occasional scans* sesuai *tier* vendor.
- **Kolaborasi lintas fungsi:** lisensi *unlimited users* memungkinkan SOC, GRC, Legal, dan Procurement bekerja pada platform yang sama tanpa hambatan akses.
- **Deteksi kebocoran eksternal:** Cyber Rank tidak hanya mengidentifikasi *data leak*, *breached credential*, dan indikasi *shadow IT* terkait vendor, tetapi juga melakukan **privacy testing berkala** agar tidak terjadi *regulatory drift*.
- **Cakupan intelijen mendalam:** **Cyber Rank does offer darknet scanning and monitoring, dengan cakupan yang sangat ekstensif.** Platform ini memiliki integrasi terbesar dengan **data breach databases dan darknet marketplace** (HIBP hanyalah salah satunya), serta **secara aktif menyisir forum daring untuk menemukan percakapan tentang potensi kebocoran data**—memberikan peringatan dini sebelum risiko menjadi insiden nyata.
- **Integrasi & otomasi:** hasil monitoring dapat diekspor langsung ke GRC/SIEM/SOAR dengan *playbook* siap pakai (misalnya: *forced reset credential leak*, *revoke OAuth*, notifikasi ke DPO). Semua aksi tercatat dalam **Remediation Tracker** lengkap dengan *owner*, *SLA*, *evidences*, dan *SOAR log*.

Kepatuhan PDP – poin penting

- **Pengendali Data** tetap memikul **liabilitas** kendati insiden terjadi di vendor; karena itu **kontrak + kontrol + pelaporan** harus *enforced* dan **dibuktikan** (scorecard, clause map, log). ([Hukumonline Learning](#))

Pelajaran kasus—krisis agregat vendor

- *CrowdStrike faulty update* (Juli 2024) memicu **outage global** lintas sektor; estimasi **kerugian agregat ≥ USD 5–10 miliar**, Delta mengklaim **> USD 500 juta** dampak langsung. **Inti:** satu *upstream vendor* bisa melumpuhkan *downstream ecosystem*. ([The Guardian](#))

Artefak bukti (operasional & manajemen risiko)

- **Quarterly Vendor Risk Review** (top risks, tren skor, rekomendasi retain/replace).
- **Remediation Tracker** tersinkron ke tiket/SOAR; **Evidence Pack** untuk rapat risiko & audit.

“What good looks like”

- **Risk-tiering vendor sejak awal** (critical / high / standard) → atur *cadence scan* (real-time untuk critical; bulanan/kuartalan untuk standard).
- **Pra-kontrak wajib:** skor risiko + privacy testing lulus; *clause map* tanpa gap kritikal (breach notice, sovereignty, audit rights, sub-processor). *Go-live* diblok jika gagal.
- **Pasca-onboarding 30–90 hari:** aktifkan alert → otomatis *SOAR action* untuk breached credential vendor; semua aksi terekam ke *Remediation Tracker*.
- **Quarterly:** Executive review + rencana substitution untuk critical vendor (antisipasi *systemic outage* ala CrowdStrike, Harvard Business Review).
- **Cyber Rank:** tidak hanya risk scoring, **Cyber Rank does offer darknet scanning and monitoring, with extremely extensive coverage**. Platform ini punya **integrasi terbesar dengan data breach databases dan darknet marketplace** (HIBP hanyalah salah satunya). Cyber Rank juga **menyisir forum daring untuk mendeteksi percakapan tentang potensi kebocoran data**, sehingga risiko bisa diidentifikasi lebih cepat sebelum insiden meluas.

Nilai terdiferensiasi Cyber Rank (vs pasar)

- **Konteks Indonesia (UU PDP):** tersedia analisis kepatuhan PDP, *privacy testing* (cookie/consent), serta deteksi klausul keamanan kontrak—fitur yang jarang ditemukan di banyak layanan rating global.
- **Efisiensi biaya:** model kredit dengan *unlimited users* membuat TCO sangat rendah untuk organisasi dengan ribuan vendor; fleksibilitas *real-time* vs *occasional scan* membantu memprioritaskan anggaran.
- **Transparansi berbasis bukti:** sertifikat yang diunggah diverifikasi dan langsung memengaruhi skor; bukan sekadar kuesioner manual yang cepat usang.
- **Cakupan intelijen yang luas:** **Cyber Rank does offer darknet scanning and monitoring, dan cakupannya sangat ekstensif**. Platform ini memiliki **integrasi terbesar dengan data breach databases dan darknet marketplace** (HIBP hanyalah salah satunya). Selain itu, Cyber Rank **juga memantau forum daring tempat pengguna membicarakan potensi kebocoran data**, sehingga organisasi

mendapatkan peringatan dini yang sulit ditiru oleh rating tools generik

Output & Bukti Audit

Cyber Rank dirancang untuk menghasilkan **artefak audit yang siap pakai**—mulai dari *scorecard* risiko vendor hingga *evidence pack* yang bisa diekspor ke sistem **GRC/SIEM** dan mendukung *governance* serta rapat manajemen risiko. Intinya, setiap temuan teknis dipaketkan menjadi materi pembuktian (*audit-ready*) yang **terstruktur, terverifikasi**, dan **dapat ditindaklanjuti**.

1. Laporan Skor Risiko Vendor (Vendor Risk Score)

- **Apa yang direkam:** Cyber Rank melakukan pemantauan **non-intrusif** atas *attack surface* publik vendor: mulai dari ekspos layanan, *vulnerabilities*, hingga indikasi *breached credentials*. Selain itu, platform juga merekam *privacy posture* vendor, seperti *policy review* maupun *cookie/consent banner assessment*. Skor risiko dibangun dengan pendekatan **dynamic updates & early warnings**, sehingga organisasi selalu mendapat sinyal terbaru terkait potensi ancaman. Lebih jauh, **Cyber Rank does offer darknet scanning and monitoring dengan cakupan yang sangat ekstensif**. Integrasinya adalah yang terbesar dengan **data breach databases** dan **darknet marketplace**—HIBP hanyalah salah satu di antaranya. Cyber Rank juga **memantau forum daring dimana pengguna mendiskusikan potensi kebocoran data**, sehingga deteksi risiko bisa dilakukan lebih cepat dibanding rating tool generik.
- **Bagaimana dipakai:**
 - **Pra-kontrak:** mendukung *go/no-go decision* dan tiering risiko (critical / high / standard).
 - **Pasca-onboarding:** menyediakan *continuous rating* untuk ribuan vendor, dengan lisensi *unlimited users* yang memfasilitasi kolaborasi lintas fungsi (SOC, GRC, Legal, Procurement).
 - **Catatan biaya (kuantitatif):** pemantauan *real-time* diposisikan sekitar ± USD/vendor/tahun. Untuk efisiensi, tersedia opsi *occasional scan* (± USD per pemindaian), sehingga organisasi bisa menyeimbangkan antara cakupan dan biaya operasional.

Nilai tambah audit: **scorecard** memperlihatkan status kepatuhan & eksposur vendor secara berkelanjutan; perubahan skor dapat ditautkan ke aktivitas korektif, sehingga memudahkan *traceability* saat audit.

2. Temuan Privasi (Privacy Findings)

- **Cakupan inti:** evaluasi **kebijakan privasi**, *cookie/consent banner*, dan indikator kepatuhan yang relevan dengan **PDP Law** (UU PDP). Fitur ini **unik** dibanding banyak platform *rating* eksternal lain karena Cyber Rank memasukkan **privacy risk detection** sebagai komponen utama.
- **Contoh keluaran:**

- **Temuan cookie/consent** (mis. *banner* tidak muncul, tidak konsisten, atau parameter *tracking* tidak sesuai).
- **Kebijakan data** yang *outdated* atau tidak mencantumkan kewajiban inti.
- Sertifikat/atribut keamanan yang **expired** (ditangkap melalui **vendor certificate detection** dan *evidence upload* yang diverifikasi).

Nilai tambah audit: daftar temuan privasi memberikan **bukti konkrit** (tangkapan hasil uji/scan, referensi halaman kebijakan) sehingga auditor dapat menilai **gap** dan **remediasi** tanpa *questionnaire* manual yang cepat kadaluarsa.

3. Remediation Tracker (SLA & Ownership)

- **Fungsi:** mengubah temuan menjadi **tindakan korektif**—siapa penanggung jawab (**owner**), **SLA**, batas waktu, dan **bukti penyelesaian** (lampiran *ticket*, log SOAR, atau pembaruan sertifikat).
- **Otomasi & integrasi:**
 - Terhubung via **API** ke **SIEM/SOAR** untuk *playbook* (mis. *credential leak* → **paksa reset, revoke OAuth, notifikasi DPO**).
 - *Sync* dengan **procurement/GRC** agar status risiko vendor masuk ke **risk register** dan mempengaruhi keputusan kontraktual.

Nilai tambah audit: *closure* setiap *issue* terikat dengan **artefak bukti** (log tindakan, cap waktu, pihak yang menyetujui)—memudahkan **pemeriksaan auditor** terhadap *effectiveness* kontrol.

4. Evidence Pack (Siap Audit)

Cyber Rank memfasilitasi pengemasan bukti agar **rapi dan dapat ditelusuri** saat *table-top*, rapat risiko, atau audit eksternal:

- **Log scan & rating updates:** catatan waktu, ruang lingkup, dan pergeseran skor.
- **Laporan insiden vendor:** notifikasi, ringkasan dampak, dan *linkage* ke aksi SOAR/SIEM.
- **Kontrak vendor + legal security clause map:** hasil deteksi otomatis klausul penting (*breach notification, data residency/sovereignty*, standar **ISO 27001/SOC 2**, hak audit, pengungkapan *sub-processor*).
- **Certificate verification log:** unggahan sertifikat vendor yang **divalidasi** dan efeknya pada skor.
- **Klasifikasi critical suppliers** (selaras persyaratan pengawasan) untuk memperlihatkan *oversight* yang proporsional.

Nilai tambah audit: *evidence pack* mempersingkat waktu *fieldwork* audit karena **bukti teknis + dokumen kontraktual** tersaji konsisten dan **dapat diekspor** ke sistem audit organisasi (GRC).

5. Integrasi & Operasionalisasi (GRC/SIEM/SOAR/Procurement)

- **Integrasi API:** menyalurkan **skor, temuan, dan status remediasi** ke **GRC** (untuk *risk governance*), **SIEM** (untuk korelasi), **SOAR** (untuk tindakan otomatis), dan **procurement** (untuk keputusan kontrak/substitusi vendor).
- **Model lisensi:** **credit-based dengan unlimited users**, memudahkan kolaborasi lintas fungsi tanpa *seat cap*—relevan saat organisasi memantau **ratusan/ribuan vendor**.
- **Pilihan pemantauan:** **real-time** atau **occasional scans** untuk menyeimbangkan prioritas risiko dan biaya.

Nilai tambah audit: integrasi memastikan **satu versi kebenaran** (*single source of truth*)—temuan teknis, kontrak, dan status remediasi **selaras** di seluruh *stakeholder*.

6. Daftar Bukti (Ringkas, siap ditempel ke *checklist* audit)

- **Vendor Risk Scorecard** (berbasis pemantauan non-intrusif + *privacy testing*).
- **Privacy Findings** (cookie/consent, kebijakan, **sertifikat expired**).
- **Remediation Tracker** (SLA, *owner*, *closure evidence*).
- **Evidence Pack:**
 - **Log scan & rating changes**
 - **Laporan insiden vendor**
 - **Kontrak + legal clause map**
 - **Certificate verification log**
 - **Klasifikasi critical suppliers**
- **Ekspor/API** ke **GRC/SIEM/SOAR/Procurement**.

7. Dampak ke UU PDP (penekanan operasional)

Walau dokumen berfokus global, Cyber Rank menegaskan dukungan **PDP Law Compliance Analysis**, *privacy posture*, dan **deteksi klausul keamanan kontrak**—praktik ini memudahkan **Pengendali Data** menunjukkan **tanggung jawab & pengawasan vendor** melalui bukti yang **audit-ready** (scorecard, clause-map, log, dan tracker). **Intinya: bukti kepatuhan yang konkret, bukan sekadar kuesioner.**

Integrasi

Cyber Rank mendukung integrasi API dengan sistem enterprise:

- **GRC:** otomatis update ke modul risk register.
- **SIEM:** korelasi alert vendor → prioritas *incident response*.
- **SOAR:** playbook auto *remediation* (misalnya *auto password reset* jika credential vendor terdeteksi di dark web).
- **Procurement system:** rekomendasi substitusi vendor jika skor risiko kritis.

Kelebihan & Keterbatasan

Kelebihan

- Konteks lokal: mendukung **UU PDP Indonesia** (analisis kepatuhan PDP Law yang tidak tersedia di Scorecard/BitSight/UpGuard).
- Skema **credit-based license** → fleksibel, biaya rendah.
- Privacy risk detection unik (cookie/consent & legal clause).
- Unlimited user license.

Keterbatasan

- Fokus pada **external/vendor risk** → bukan pengganti DLP/DSPM harian di internal sistem.
- **Market share** masih regional (belum global).
- Komunitas pendukung lebih kecil dibanding BitSight/Scorecard.

Checklist Implementasi Cepat (4 Minggu)

Minggu 1: Persiapan

- Identifikasi 20 vendor kritikal (berbasis data flow UU PDP).
- Daftarkan vendor ke dashboard Cyber Rank.

Minggu 2: Audit Awal

- Jalankan scan risiko eksternal (attack surface, cookie, breach).
- Upload kontrak vendor → deteksi klausul keamanan otomatis.

Minggu 3: Integrasi

- Hubungkan output ke SIEM/GRC internal.
- Rancang playbook dasar di SOAR (credential leak → reset otomatis).

Minggu 4: Reporting & Review

- Hasilkan laporan kepatuhan PDP untuk manajemen risiko.
- Bentuk *remediation tracker* → follow-up dengan vendor.
- Susun *evidence pack* → siap dipakai audit eksternal/LAM-Infokom.

Kesimpulan

Cyber Rank adalah solusi **praktis & kontekstual Indonesia** untuk mengelola risiko eksternal/vendor dalam kerangka UU PDP.

- **Jika target utama:** *kepatuhan & vendor risk* → Cyber Rank jadi jangkar.
- **Jika fokus:** *kontrol teknis internal* → butuh kombinasi dengan DSPM/DLP (BigID, Securiti).
- **Jika early warning breach intel** → dipasangkan dengan DarkRadar.io.

Dengan biaya rendah dan konteks regulasi Indonesia, Cyber Rank menawarkan **jalan cepat menuju compliance PDP** tanpa beban lisensi global yang mahal.

BAB 6: DarkRadar.io Threat Intelligence

DarkRadar.io (juga dikenal sebagai **Dark Radar**) memposisikan diri sebagai solusi *cyber threat intelligence* yang berfokus pada *dark web monitoring*, pemantauan kebocoran data (breach), dan *alerting* terhadap paparan domain, email, atau merek organisasi.

(darkradar.io)

Beberapa metrik yang dipublikasikan secara resmi:

- Data yang dianalisis: **300 miliar lebih** (total *analysed data*) (darkradar.io)
- Akun yang pernah terkena breach yang terdeteksi dalam basis mereka: **85 miliar+** (darkradar.io)
- Dalam konteks lokal, DarkRadar pernah mengumumkan bahwa lebih dari **1.000 situs .go.id** tercatat diretas atau terdampak kebocoran (menurut posting LinkedIn) ([LinkedIn](#))

Dari sudut pandang teknis, DarkRadar beroperasi sebagai “canary” bagi organisasi, memantau aktivitas di lapisan tersembunyi (forum gelap, pasar kriminal, chat tersembunyi, *stealer logs*, dan sebagainya) dan memberi sinyal awal bahwa data organisasi mungkin telah diekspos atau dijual.

Dalam perspektif threat intelligence umum, *dark web monitoring* adalah bagian dari sistem peringatan dini yang terus-menerus mencari jejak kompromi seperti kredensial bocor, metadata terkait (IP, domain, hash), ataupun diskusi kriminal yang menyebut nama organisasi atau karyawan. (crowdstrike.com)

Fitur Inti & Fungsi Operasional

Di balik narasi pemasaran, fungsi-fungsi berikut harus menjadi sorotan teknis dan audit:

1. **Pemantauan Domain / Email / Merek (Brand Monitoring)**
 - Mencari penyebutan merek, nama entitas, domain/subdomain, atau email yang terasosiasi organisasi di forum underground, chat tersembunyi, marketplace kriminal.
 - Mendeteksi domain spoofing atau domain lookalike yang disebutkan oleh aktor ancaman sebagai vektor phishing/penipuan.
2. **Breach Intelligence (Inteligensi Kebocoran)**
 - Mendeteksi apakah data organisasi (atau milik karyawan) sudah muncul di basis data kebocoran umum atau pasar gelap.
 - Memanfaatkan *stealer logs*, dump database, file korban ransomware, data dump di pasar gelap sebagai sinyal kebocoran.
 - Melacak tren ransomware, permintaan tebusan, dan interaksi kelompok kriminal. (darkradar.io)
3. **Alerting / Notifikasi & Prioritisasi**

- Menghasilkan alert real-time atau mendekati real-time terhadap temuan yang relevan.
- Menyajikan *context enrichment* — misalnya: lokasi asal, forum, poster asli, tanggal, bukti pendukung.
- Mengelompokkan prioritas (misalnya, kredensial aktif vs data dump lama vs diskusi spekulatif).

4. Threat Hunting & Diskusi Hacker Tracker

- Memantau forum, chat, grup tersembunyi, diskusi antar aktor kriminal, untuk mencari indikasi kampanye, rencana, atau target baru. (darkradar.io)
- Mengumpulkan *indirect intelligence* seperti narasi pelaku, metode, ransomware chain, target industri, dan modus operandi.

5. Skalabilitas & Infrastruktur Data

- Menangani volume data massif dari web gelap, forum, marketplace, dan log eksternal — ini menuntut infrastruktur crawling, ekstraksi, pemfilteran, dan korelasi.
- Sistem pembobotan *noise filtering* agar alert relevan tidak tenggelam oleh data “sampah.”

6. Integrasi API / Ekspor

- Menyediakan API atau konektor agar data intel (IOC feed, metadata, alert) bisa diekspor ke sistem luar (SIEM, SOAR, platform intel eksternal).

Kasus Penggunaan / Use Cases Kritis

Berikut beberapa skenario praktis di mana DarkRadar.io (atau solusi *dark-web intel* serupa) berpotensi memberikan nilai kritis:

Use Case	Penjelasan	Nilai Tambah & Catatan
Deteksi Kredensial Bocor	Ketika kredensial pekerja (email + password) muncul di <i>stealer log</i> atau dump database, alert bisa memicu tindakan mitigasi lebih cepat.	Mengurangi risiko <i>account takeover / lateral movement</i> . Namun deteksi sering <i>late stage</i> — bisa saja setelah penyerang sudah menggunakan data.
Pemantauan Executive Impersonation	Merek atau nama pejabat organisasi muncul di forum kriminal atau penipuan → indikasi phish atau impersonasi.	Dapat mencegah spear-phishing atau penipuan reputasi.
Attack Surface Exposure Underground	Mendeteksi subdomain internal, versi aplikasi, server lembah (shadow IT), host yang disalahgunakan — muncul di web gelap.	Menjadi early warning untuk memperkuat atau menutup celah.

Rencana & Kampanye Aktor Ancaman	Diskusi internal pelaku di forum tentang target, teknik, potensi serangan ke industri/sektor Anda.	Bisa jadi lead bagi tim <i>threat hunting</i> atau intel internal.
Keterkaitan ke Insiden Vendor / Mitra	Kebocoran data di vendor X yang memuat data Anda bisa terdampak → alert dari DarkRadar menjadi sinyal supaya Anda cek exposure di rantai pasok.	Berguna untuk manajemen risiko vendor (vendor risk).

Dalam praktik komunitas, terdapat skeptisisme bahwa *dark web monitoring* kadang terlalu banyak *noise* dibanding sinyal yang actionable. Seorang pengguna di forum cybersecurity menulis:

“Actionable intel is gonna be there if your organization is large ... but you will filter through a lot of their noise.” ([Reddit](#))

Jadi peran tim keamanan internal sangat penting dalam menyaring false positive dan menentukan tindakan.

Integrasi & Otomasi di Arsitektur Keamanan

Untuk menjadikan DarkRadar.io bukan sekadar tool pengawasan pasif, integrasi dan otomasi harus menjadi kunci:

- **SIEM / Platform korelasi**
Koneksikan alert ke SIEM (Splunk, Azure Sentinel, Wazuh, dsb.). Setiap alert dari DarkRadar menjadi event yang bisa dikorelasi dengan log internal (login, IAM, EDR) untuk mendeteksi eskalasi.
- **SOAR / Orkestrasi Respon**
Bangun *playbook* yang otomatis menindak alert-level tinggi:
 - Reset password akun (jika kredensial dicurigai).
 - Revoke OAuth / token akses yang terkait.
 - Kirim notifikasi ke DPO / tim compliance.
 - Buat tiket insiden / eskalasi ke tim forensik internal.
- **Automated Enrichment / Lookup**
Alert dapat diperkaya dengan lookup tambahan: pemetaan ke pengguna internal, cross-check ke logs event login, reputasi IP, geolokasi, dsb.
- **Feedback loop**
Hasil respon (misalnya, kredensial terbukti aktif / tidak) harus dikembalikan sebagai *feedback* ke sistem scoring alert / mesin filter, agar false positive dikurangi dari waktu ke waktu.
- **Integrasi ke GRC / Compliance**
Ekspor ringkasan insiden ke modul GRC / audit internal agar dapat digunakan sebagai bukti mitigasi terkait UU PDP atau audit keamanan.

Output & Bukti Audit

Untuk keperluan audit (terutama di ranah UU PDP atau standar keamanan), output berikut dari DarkRadar.io perlu dikumpulkan dan diverifikasi:

- **Laporan Intel (Threat Intelligence Report)**
Analisis naratif: kapan dan bagaimana kebocoran muncul, actor ancaman, modus, dampak potensial.
- **IOC Feed / Daftar Indikator Kompromi (hash, IP, domain, email)**
Format machine-readable (STIX, CSV, JSON) yang dapat digunakan untuk integrasi SIEM / deteksi aktif.
- **Catatan Korelasi (Correlation Notes / Contextual Notes)**
Untuk setiap alert: metadata seperti forum asal, poster, waktu, bukti pendukung (screenshot, link, kutipan), serta analisis relevansi.
- **Timeline Insiden**
Urutan kronologis: waktu deteksi, eskalasi, mitigasi, validasi.
- **Catatan Aksi / Respon**
Log tindakan otomatis (reset password, revoke token, notifikasi) dan aksi manual (verifikasi, investigasi).
- **Estimasi Dampak / Skala Eksposur**
Perkiraan jumlah akun yang terpapar, data jenis apa (PII, kredensial, finansial), segmentasi berdasarkan tingkat keparahan.
- **Log Integrasi / Ekspor**
Bukti bahwa data alert telah berhasil masuk ke SIEM/SOAR/GRC (timestamp, ID integrasi).

Bukti di atas sangat berguna untuk auditor keamanan, tim audit internal, maupun kewajiban pelaporan insiden di UU PDP.

Kelebihan & Keterbatasan (Analisis Kritis)

Kelebihan:

- Memberi *early warning* terhadap kebocoran eksternal yang belum terdeteksi lewat sistem internal.
- Mendapat visibilitas ke ruang kriminal underground yang tidak dapat dijangkau melalui Tool keamanan tradisional.
- Menjadi Tool korelasi untuk memperkaya intel internal dan prioritas respon.
- Dengan integrasi otomatis, bisa mempersingkat *dwell time* atau waktu eksposur risiko yang tidak diketahui.
- Dapat memperkaya bukti mitigasi dalam konteks audit dan kepatuhan (meskipun bukan menggantikan framework kepatuhan).

Keterbatasan:

- **Tidak dirancang untuk kepatuhan regulasi secara penuh** — misalnya, ia tidak menggantikan kerangka keamanan internal, DLP, DSPM, atau kebijakan privasi.

- **False positive & noise tinggi** — banyak alert yang bersifat historis, data lama, atau tidak relevan dengan konteks organisasi.
- **Ketergantungan pada kemampuan crawling / akses ke forum gelap** — data gelap sangat dinamis, forum ditutup atau berpindah, dan churning tinggi. Misalnya, studi menyebutkan onion domain tumbuh drastis (20× dalam 5 tahun) dan churn tinggi. ([arXiv](#))
- **Perlu korelasi internal** — Temuan dari DarkRadar harus diverifikasi dan dikorelasi dengan data internal agar menjadi aksi nyata, tidak cukup “alert saja.”
- **Keterbatasan cakupan** — Tidak semua kebocoran terekam atau diunggah ke forum publik; actor ancaman bisa menggunakan jalur tertutup.
- **Biaya & skala** — Untuk organisasi kecil, cost vs return bisa sulit dibenarkan. Tools intel semacam ini sering lebih bernilai di organisasi besar atau dengan profil risiko tinggi.

Playbook Respons 24 Jam (Contoh Langkah-demi-langkah)

Berikut sebuah *sketsa playbook* 24 jam yang dapat Anda adaptasi dan integrasikan ke SOAR / SOP internal:

Waktu & Fase	Langkah	Catatan / Kontrol
T+0 (Deteksi)	Alert DarkRadar masuk ke SIEM / SOAR	Filter berdasarkan prioritas (misalnya: kredensial aktif > dump lama)
T+15 menit	Enrichment otomatis: lookup ke AD/LDAP, periksa login terakhir, reputasi IP	Jika kredensial user ditemukan, cek aktivitas login abnormal
T+30 menit	Validasi <i>false positive</i> — tim keamanan memeriksa bukti, metadata, konteks	Tandai yang benar-benar relevan
T+45 menit	Untuk kredensial aktif: otomatis reset password / revoke token	Kirim notifikasi ke pengguna & tim keamanan
T+1 jam	Escalasi ke tim forensik: cek apakah ada akses tak sah menggunakan kredensial tersebut	Audit log, EDR, IAM logs
T+2–4 jam	Cross-check dampak: identifikasi data internal yang dapat diakses dengan kredensial itu (jika memungkinkan)	Segmentasi potensi eksposur
T+4 jam	Susun draft laporan insiden internal (format INTEL)	Lampirkan bukti awal, timeline, rekomendasi mitigasi

T+6 jam	Kirim pemberitahuan formal ke DPO / tim compliance / manajemen (jika relevan per UU PDP)	Sertakan estimasi awal jumlah akun/data terpapar
T+8 jam	Mulai langkah mitigasi tambahan (misal, forcing MFA, verifikasi ulang login, audit akses)	Pastikan kredensial lama tidak dapat dipakai kembali
T+12 jam	Review respon: adakah aktivitas residual, alert lanjutan, koreksi false negative	Update playbook bila ada gap
T+24 jam	Finalisasi laporan insiden, ringkasan tindakan & mitigasi, lessons learned	Jadwalkan debrief internal dan update SOP

Catatan: semua waktu bersifat target ideal; organisasi harus menyesuaikan dengan SLA, ketersediaan tim, dan kapasitas integrasi.

Posisi DarkRadar.io dalam Lanskap Tool dalam Buku Ini

Dalam struktur buku Anda, DarkRadar.io berperan sebagai lapisan *early warning / external leak detection*, bukan sebagai Tool kontrol internal semata. Ia melengkapi (bukan menggantikan) DSPM, DLP, EDR, dan mekanisme pemantauan internal.

Dalam tabel perbandingan Tool (BAB 8), baris untuk DarkRadar.io bisa seperti:

Tool	Kategori	Auto PII Discovery	Data Leak (SaaS/Email/Code)	Password Leak Check	Dark-Web Monitoring	Auto Advice/Remediate	Compliance Reporting	Integrasi	Estimasi Biaya / Tier
DarkRadar.io	Dark-Web Intel	—	insiden kebocoran terindikasi	Ya	Ya (intiproduk)	Melalui SOAR / playbook	Template insiden	SIE M, SOA R, API	\$\$

Dalam roadmap implementasi (BAB 11), fase integrasi DarkRadar biasanya menyusul setelah assessment & pilot (bulan 3–4) dan digabungkan ke arsitektur integrasi (bulan 5–6), lalu diuji UAT (bulan 7–8) sebagaimana dijelaskan.

Catatan Penutup & Rekomendasi untuk Praktisi IT

- Jangan memposisikan DarkRadar.io sebagai *silver bullet*; ia adalah bagian dari *defense-in-depth* yang mengandalkan kolaborasi tim, konteks, dan korelasi internal.

- Uji coba *pilot* di cakupan terbatas (misalnya, hanya domain penting) untuk mengevaluasi rasio false positive vs nilai aksi nyata di lingkungan organisasi Anda.
- Pastikan *feedback loop* agar alert yang terbukti tidak relevan tidak terus-menerus memicu noise.
- Untuk audit UU PDP, tambahkan bukti bahwa organisasi memantau potensi eksposur eksternal (sebagai langkah kewajiban keamanan — *due diligence*).
- Selalu padukan intel dark web dengan kontrol teknis (MFA, DLP, IAM hygiene, enkripsi, segmentasi) agar tidak menjadi “alarm tanpa action.”

BAB 7: Panorama Pasar: Privacy/DSPM/DLP, OSS, OSINT & Identity Exposure

Snapshot Eksekutif (apa yang penting untuk IPT/IT Ops)

- **Privacy/DSPM/DLP komersial:** kuat untuk *auto-discovery* PII, *policy enforcement*, & pelaporan kepatuhan (GDPR/ISO)—**namun biaya dan kompleksitas tinggi**. Purview & Google DLP menempel ketat di ekosistem cloud; BigID/Securiti unggul pada DSPM lintas *hybrid-multicloud*. ([TrustArc](#))
- **Open-source (Wazuh/Suricata, TruffleHog/Gitleaks):** fleksibel, murah, **butuh tuning** & integrasi (SIEM/SOAR) untuk menurunkan *false positive* dan menjadi bukti audit yang rapi. ([Dokumentasi Wazuh](#))
- **OSINT dark-web & otomasi (Ahmia/OnionScan, n8n):** mendukung *threat intel* & *evidence enrichment*, bukan pengganti kontrol inti; kuat untuk *playbook near-real-time*. ([ahmia.fi](#))
- **Identity exposure (HIBP/SpyCloud):** indikator kredensial/identitas bocor untuk kebijakan sandi & *account-takeover*—*must-have* sebagai sinyal eksternal. Per Sept 2025, **HIBP** menampilkan **15,1 miliar+ akun**; **SpyCloud** melaporkan **63,8 miliar distinct identity records** yang “direkap” dari darknet (+24% YoY). **Angka ini menjustifikasi otomatisasi reset/revoke** via SOAR. ([Have I Been Pwned](#))

Inti: **gabungkan** DSPM/DLP (kontrol internal) + **dark-web/identity intel** (sinyal eksternal) + **SIEM/SOAR** (korelasi & aksi). Itu yang paling *audit-friendly* untuk UU PDP.

Commercial Privacy/DSPM/DLP

OneTrust (PrivacyOps & Data Mapping)

- **Peran:** *Privacy operations suite* untuk *data mapping*, RoPA, PIA/DPIA, *vendor risk*, & orkestrasi kepatuhan.
- **Kenapa relevan ke UU PDP:** *Mapping* aktivitas pemrosesan + *assessment* jadi *artefak audit* yang kuat (lampirkan RoPA, DPIA).
- **Catatan:** *Privacy automation* fokus mengurangi beban manual; rilis 2025 menambah *inventory review* untuk perubahan otomatis. ([onetrust.com](#))

BigID (DSPM/Data Discovery)

- **Peran:** *AI-powered discovery & classification* lintas *cloud/on-prem/SaaS*; unggul pada *contextual/identity-aware classification*.
- **Nilai:** Menekan risiko *shadow data* & mempermudah *linkage* data-subjek (DSR).
- **Catatan:** Blog & *market guide* 2024–2025 menekankan cakupan ratusan konektor & *risk analysis* proaktif. ([BigID](#))

Securiti.ai (Data Command Center / DSPM)

- **Peran:** *Data+AI Intelligence* & kontrol lintas *hybrid-multicloud*; *Data Command Graph* untuk konteks objek data/AI.
- **Nilai:** *Unified platform* (security, governance, privacy); kuat untuk organisasi multinasional.
- **Catatan:** Dinilai tinggi di liputan industri 2025. ([Securiti](#))

Microsoft Purview (DLP di M365/Windows/Endpoint)

- **Peran:** *Policies* DLP untuk **data-at-rest/in-motion/in-use** di Microsoft 365, endpoint, dan *services* terkait.
- **Nilai:** *Native enforcement* (labeling, *exfil control*, *activity monitoring*) + integrasi *compliance*.
- **Catatan:** Dokumentasi 2025 menegaskan cakupan lokasi & aktivitas pengguna. ([Microsoft Learn](#))

Google Cloud DLP / Sensitive Data Protection

- **Peran:** Deteksi/masking PII via **ratusan *infoTypes*** (*built-in* + *custom*). **Termasuk *INDONESIA_PASSPORT*** sejak Okt 2024—relevan untuk konteks lokal.
- **Nilai:** *De-identification* (redaction, masking, FPE) + integrasi di *pipelines*.
- **Catatan:** Referensi *infoTypes* & *release notes* menguatkan dukungan regional yang makin kaya. ([Google Cloud](#))

Symantec DLP (Broadcom)

- **Peran:** *Enterprise-grade DLP* (EDM, *fingerprinting*, ML), *endpoint/network/cloud*; *response actions* termasuk karantina/flag.
- **Nilai:** Matang untuk organisasi besar & *regulated*.
- **Catatan:** Rilis 25.1 & *product brief* menyorot deteksi konten canggih & *cloud detection service*. ([TechDocs](#))

Kritik singkat: Solusi komersial **kuat pada *completeness***, namun **perlu waktu adopsi** (data-source onboarding, *tuning* klasifikasi) dan **biaya/TCO** sering menjadi kendala, terutama di Pemda/RS pendidikan.

Open-Source / Community

Wazuh (XDR/SIEM) + Suricata (NIDS/NIPS/NSM)

- **Peran:** Wazuh sebagai **SIEM/XDR OSS** + *agent* serbaguna; Suricata sebagai **NIDS/IPS/NSM** dengan *full-pcap*, *TLS cert logging*, *file extraction*.
- **Kegunaan PDP:**
 - **Wazuh:** korelasi *events*, *file integrity monitoring*, *compliance checks*, jadi *hub* untuk log & *rule hits* PII.
 - **Suricata:** *network-level rules* untuk *data exfil* & pola PII (regex) → bukti *prevent/detect*.

- **Dokumentasi/fitur:** instalasi & arsitektur *current*; fitur Suricata *NSM beyond IDS*. ([Dokumentasi Wazuh](#))

TruffleHog / Gitleaks (Secrets & Repo Leaks)

- **Peran:** *Secret scanning* di *git history*, file & *stdin*.
- **Fakta:** TruffleHog klaim **>800 tipe secret** dan **validasi *live***; Gitleaks: OSS *secret scanner* dgn **14M+ GitHub downloads & 20M+ Docker pulls**.
- **Kegunaan PDP:** temuan *token/API key/credential* → *immediate revoke* via SOAR; log scan jadi **artefak audit**. ([GitHub](#))

OSINT Dark-Web & Otomasi

Ahmia & OnionScan

- **Ahmia:** *Search engine* untuk layanan *.onion* (akses via Tor); berguna sebagai *starting point* investigasi. ([ahmia.fi](#))
- **OnionScan:** Tool untuk memeriksa *misconfiguration* dan *opsec leaks* pada *hidden services*—bermanfaat untuk *threat intel* & edukasi tim. ([GitHub](#))

n8n (Workflow/Otomasi)

- **Peran:** *source-available* otomasi *drag-n-drop* yang **ideal mengikat HIBP/SpyCloud/DarkRadar** → SIEM/SOAR (webhook → enrich → *ticketing* → notifikasi DPO).
- **Catatan:** Dirancang untuk *self-host* atau cloud; populer di komunitas *self-hosted*. ([n8n](#))

Kritik: OSINT & otomasi **bukan kontrol**—mereka ***multiplier*** untuk memperkaya konteks & mengeksekusi *playbook*. Butuh *guardrails* (akses, logging, *rate-limit*).

Identity Exposure (Password/Kredensial)

Have I Been Pwned (HIBP)

- **Fakta terbaru** (homepage): **15.107.305.775** akun “**pwned**” terindeks; **907** *paste records*.
- **Praktik:** gunakan API untuk *password policy* (*block known-compromised*), *email watch*, & *user notification*. ([Have I Been Pwned](#))

SpyCloud

- **Fakta tren 2025:** **63,8 miliar** *distinct identity records* yang “direkap” (naik **24% YoY**); banyak org **tidak otomatis reset/revoke** setelah phishing/malware (hanya **~41–54%**).

- **Implikasi:** *Identity-centric response* + **otomasi** (SOAR) **sangat disarankan**. ([PR Newswire](#))

Konklusi kebijakan sandi: **Blok reuse** sandi yang pernah bocor, **paksa MFA**, dan **otomasi reset/revoke** saat *indicator* muncul dari HIBP/SpyCloud/DarkRadar. Ini *low-hanging fruit* yang **terukur dampaknya** pada MTTR.

Pemetaan Singkat ke UU PDP (apa yang jadi artefak?)

- **Privacy/DSPM/DLP** (OneTrust/BigID/Securiti/Purview/Google DLP/Symantec DLP)
 - *Artefak: data map/RoPA, PIA/DPIA, sensitive data inventory, policy hits, incident report.*
- **OSS (Wazuh/Suricata)**
 - *Artefak: rule hits, FIM logs, network alerts, pcap extracts, correlation di SIEM.*
- **Repo Scanners (TruffleHog/Gitleaks)**
 - *Artefak: scan logs, secret IDs, ticket revocation, commit remediation evidence.*
- **OSINT & Identity (Ahmia/OnionScan/HIBP/SpyCloud)**
 - *Artefak: intel report, IOC feed, identity exposure list, SOAR action logs (reset/revoke/notify DPO).*

Catatan Kritis & Rekomendasi Implementasi

- **Jangan “tool-centric”:** susun alur *Discover* → *Classify* → *Protect* → *Detect* → *Respond* → *Report* (BAB 3) dan pilih tool **untuk mengisi celah**.
- **Mulai dari sinyal bernilai-aksi:**
 - **DSPM/DLP** untuk *reduksi attack surface data* (internal).
 - **HIBP/SpyCloud/DarkRadar** untuk **peringatan eksternal** (leak/kredensial).
 - **Wazuh/Suricata** untuk **korelasi & network-level controls**.
- **Otomasi minimal** (bisa dikerjakan tim kecil):
 - *Webhook intel* → **SIEM** → **SOAR** → aksi: **reset password, revoke token OAuth, notifikasi DPO + pembuatan tiket** (tercatat sebagai **bukti audit**).
- **Angka yang perlu “menyadarkan” manajemen:**
 - HIBP **15,1 miliar akun pwned**; SpyCloud **63,8 miliar** identitas terekap (**+24% YoY**) ⇒ **risiko credential-stuffing & ATO sangat nyata** bila tidak ada *compromised-password policy + automated remediation*. ([Have I Been Pwned](#))

Daftar Sumber Kunci (untuk due diligence cepat)

- **DarkRadar.io** — *dark web monitoring / hacker discussion tracker*. (darkradar.io)
- **BigID** — DSPM (*discovery/classification/AI*). ([BigID](https://bigid.ai))
- **Securiti.ai** — *Data Command Center / DSPM*. ([Securiti](https://securiti.ai))
- **OneTrust** — PrivacyOps (RoPA, PIA/DPIA, vendor risk, *automation*). (onetrust.com)
- **TrustArc** — *Assessment Manager* (PIA/DPIA/TIA/vendor). ([TrustArc](https://trustarc.com))
- **Microsoft Purview DLP** — *policies data-at-rest/in-motion/in-use*. ([Microsoft Learn](https://microsoft.com/learn))
- **Google Sensitive Data Protection (DLP)** — *infoTypes & update INDONESIA_PASSPORT* (Okt 2024). ([Google Cloud](https://cloud.google.com/dlp))
- **Symantec DLP (Broadcom)** — *enterprise DLP*, rilis 25.1. ([Broadcom](https://broadcom.com))
- **Wazuh** — OSS XDR/SIEM; dokumentasi & instalasi. ([Dokumentasi Wazuh](https://wazuh.com))
- **Suricata** — IDS/IPS/NSM, *features*. ([Suricata](https://suricata.io))
- **TruffleHog** — **>800** tipe secret + **live validation**. ([GitHub](https://github.com))
- **Gitleaks** — OSS *secret scanner* populer (14M+ GitHub downloads, 20M+ Docker pulls). ([Gitleaks](https://gitleaks.io))
- **Ahmia** — *Tor hidden services search*. (ahmia.fi)
- **OnionScan** — audit kebocoran *opsec hidden services*. ([GitHub](https://github.com))
- **n8n** — *source-available workflow automation* (self-host/cloud). ([n8n](https://n8n.io))
- **HIBP** — **15,1 miliar+** akun *pwned* (homepage, akses publik). ([Have I Been Pwned](https://haveibeenpwned.com))
- **SpyCloud** — **63,8 miliar** *distinct identity records* direkap (2025). ([PR Newswire](https://prnewswire.com))

Bonus ringkas (untuk slide)

- **If target utama kepatuhan** → **OneTrust/TrustArc + Purview/Google DLP/Symantec** (*pelaporan & control enforcement*).
- **Jika target pengendalian data teknis** → **BigID/Securiti (DSPM) + DLP**.
- **Jika target *early warning* kebocoran** → **DarkRadar.io + HIBP/SpyCloud** (+ n8n/SOAR untuk *auto reset/revoke*).
- **Jika *budget-ketat*** → **Wazuh + Suricata + Gitleaks/TruffleHog** (*rule-based evidence + ticketing*).

BAB 8: Perbandingan Tools

Bab ini menyajikan perbandingan mendalam antara lima kategori utama tool yang relevan untuk audit privasi data dan kepatuhan UU PDP. Setiap tool dibedah dari sisi fungsi, kekuatan, keterbatasan, serta estimasi biaya.

Cyber Rank – Fokus Compliance dan Vendor Risk

Cyber Rank menempati posisi unik sebagai platform yang berorientasi pada **kepatuhan** dan **manajemen risiko pihak ketiga**. Berbeda dengan DLP atau DSPM yang bersifat teknis, Cyber Rank menghasilkan **skor kepatuhan vendor** serta analisis risiko yang disesuaikan dengan konteks Indonesia.

- **Kelebihan utama:**
 - Kontekstual dengan **UU PDP**, termasuk *due diligence* pada vendor lokal.
 - **Laporan siap audit** yang bisa diekspor langsung ke GRC atau SIEM.
 - Memberikan **rekomendasi kebijakan** serta langkah mitigasi risiko yang praktis.
 - **Cyber Rank juga menawarkan darknet scanning and monitoring dengan cakupan yang sangat luas.** Platform ini memiliki **integrasi terbesar dengan database kebocoran data dan darknet marketplace** (HIBP hanyalah salah satunya), serta **memantau forum daring** di mana pengguna membicarakan potensi kebocoran data. Fitur ini memberi nilai tambah besar dibanding rating tool generik.
- **Keterbatasan:**
 - Tidak melakukan *auto-discovery* PII di lingkungan internal.
 - Tidak berfokus pada deteksi kebocoran data di SaaS atau email.
- **Estimasi biaya:** relatif terjangkau, di kisaran \$–\$\$ tergantung pada jumlah vendor yang dipantau.

Dengan karakteristik ini, Cyber Rank tepat untuk organisasi di Indonesia yang ingin **memperkuat bukti kepatuhan**, khususnya dalam **audit vendor dan kontrak mitra**.

DarkRadar.io – Early Warning Dark-Web & Breach Intel

DarkRadar.io merupakan solusi intelijen yang berfokus pada **dark-web monitoring dan breach intelligence**. Tool ini memberikan **peringatan dini** terhadap kredensial bocor, impersonasi eksekutif, dan aktivitas grup ransomware.

- **Kelebihan:**
 - Monitoring domain/email/brand di ranah underground.
 - IOC feed dan laporan insiden yang bisa langsung diintegrasikan dengan SIEM/SOAR.
 - Mendukung playbook otomatis, misalnya reset password atau revoke token.
- **Keterbatasan:**

- Tidak melakukan scanning internal atau auto-discovery PII.
- Bergantung pada coverage intel; potensi blind spot tetap ada.
- **Estimasi biaya:** \$\$ (kelas menengah, berbasis subscription intel).

DarkRadar.io ideal sebagai lapisan “eksternal”, melengkapi DLP/DSPM, untuk mendeteksi kebocoran lebih cepat.

BigID / Securiti – DSPM & DLP Premium

BigID dan **Securiti** adalah contoh solusi kelas enterprise dalam kategori **DSPM/DLP (Data Security Posture Management / Data Loss Prevention)**. Mereka unggul dalam **auto-discovery PII** dengan teknologi machine learning, serta mendukung integrasi lintas cloud dan SaaS.

- **Kelebihan:**
 - Auto-discovery PII di database, cloud storage, SaaS, hingga repo code.
 - Enforcement kebijakan otomatis, termasuk playbook remediasi.
 - Integrasi luas dengan API, SIEM, dan SOAR.
 - Bisa dimapping ke GDPR/CCPA, lalu *customized* untuk UU PDP.
- **Keterbatasan:**
 - Kompleksitas deployment tinggi, memerlukan tim khusus.
 - Biaya sangat tinggi, \$\$\$ (enterprise tier).

Solusi ini cocok untuk **enterprise berskala besar** atau sektor regulated (fintech, perbankan, kesehatan) yang membutuhkan cakupan penuh dan integrasi global.

Wazuh – OSS SIEM Fleksibel

Wazuh adalah platform **open-source SIEM** yang memberikan fleksibilitas tinggi bagi organisasi dengan anggaran terbatas. Dengan dukungan rule dan regex, Wazuh dapat dimanfaatkan untuk mendeteksi pola kebocoran data dan integrasi dengan *custom PII detector*.

- **Kelebihan:**
 - Gratis (OSS), biaya hanya pada infrastruktur dan SDM.
 - Integrasi luas dengan Suricata, Elastic, TheHive, Shuffle.
 - Cocok sebagai pondasi SIEM di institusi pendidikan, pemda, atau BUMN dengan budget ketat.
- **Keterbatasan:**
 - Tidak ada modul dark-web native.
 - Butuh tuning intensif dan SDM teknis yang berpengalaman.
- **Estimasi biaya:** \$ (hanya infrastruktur + tim).

Wazuh memberi keseimbangan antara *low-cost* dan fleksibilitas, meski tidak sekuat DSPM komersial.

TruffleHog & Gitleaks – Secrets Scanner untuk DevSecOps

TruffleHog dan **Gitleaks** adalah tool open-source yang fokus pada **secrets scanning** di repositori kode. Mereka menjadi bagian vital dalam pipeline **DevSecOps** untuk mencegah bocornya API keys, token, atau kredensial sensitif di Git.

- **Kelebihan:**
 - Ringan dan cepat diintegrasikan pada CI/CD pipeline.
 - Efektif mencegah *supply chain leak* yang sering diabaikan.
 - Gratis, dengan komunitas aktif.
- **Keterbatasan:**
 - Fokus terbatas pada code repositori; tidak bisa scanning PII di storage/email.
 - Output berupa log, sehingga perlu integrasi tambahan untuk reporting formal.
- **Estimasi biaya:** \$ (open-source, hanya biaya pipeline).

Tool ini relevan untuk organisasi dengan aktivitas development aktif, terutama startup atau software house.

Ringkasan Eksekutif

Dari analisis di atas, dapat diringkas:

- **Cyber Rank** unggul pada **kepatuhan UU PDP & vendor risk**.
- **DarkRadar.io** memberi **early warning** kebocoran di dunia bawah tanah.
- **BigID/Securiti** adalah solusi **premium enterprise** dengan cakupan menyeluruh.
- **Wazuh** menjadi alternatif **OSS SIEM** yang ekonomis namun butuh tuning.
- **TruffleHog/Gitleaks** melengkapi dari sisi **DevSecOps** untuk mencegah kebocoran secrets di codebase.

Dengan demikian, kombinasi optimal harus disesuaikan dengan **profil organisasi**:

- **Startup fintech** → DarkRadar.io + DSPM ringan + TruffleHog.
- **BUMN/RS pendidikan** → Cyber Rank + Wazuh + script lokal.
- **Enterprise multinasional** → BigID/Securiti + DarkRadar.io + Cyber Rank.

BAB 9: Arsitektur Integrasi & Otomasi (SOAR-Centric)

Organisasi modern tak lagi cukup mengandalkan *siloed tools*. Yang dibutuhkan adalah **jalur pipa end-to-end**: *sinyal* → *korelasi* → *aksi* → *bukti audit*. Desain yang baik memadukan **kontrol internal** (DSPM/DLP, EDR), **intel eksternal** (DarkRadar.io, HIBP/SpyCloud), **korelasi** (SIEM), dan **otomasi respons** (SOAR). Hasil akhirnya bukan hanya penurunan *MTTD/MTTR*, tetapi juga **artefak audit otomatis** yang siap diuji terhadap **UU PDP**.

Referensi Arsitektur (Sinyal → Korelasi → Aksi)

Sinyal (Deteksi & Intel):

- **DSPM/DLP**: *auto-discovery* PII & kebijakan *data handling* di SaaS/DB/storage.
- **DarkRadar.io**: *real-time dark-web & breach intelligence* (forum bawah tanah, *stealer logs*, ransomware leak sites) untuk *early warning* paparan domain/email/brand. Ini memang posisi inti DarkRadar (modul: *Threat Hunting, Hacker Discussion Tracker, Employee Data Breach, Stealer Logs, Ransomware Activity Monitoring*). (darkradar.io)
- **HIBP**: *password exposure check* via **k-anonymity API** (hash SHA-1; hanya 5 karakter awal yang dikirim), aman untuk *policy enforcement*. Saat ini memuat **15,1+ miliar** akun terekspos. ([Have I Been Pwned](https://haveibeenpwned.com))
- **SpyCloud**: *recaptured darknet data* skala besar; **53,3 miliar distinct identity records** (naik **22% YoY**). Temuan tipikal: **52 username/141 pasangan kredensial per individu** di data terekspos—indikasi serius bagi kontrol identitas. ([SpyCloud](https://spycloud.com))

Korelasi (SIEM):

- **Wazuh / Microsoft Sentinel / Splunk** mengagregasi log & alert (DSPM/DLP, DarkRadar, HIBP/SpyCloud, EDR), menghubungkan *who/what/when* lintas sumber, dan menyiapkan case insiden untuk SOAR. (Deskripsi peran umum SIEM.)

Aksi (SOAR):

- Otomasi respons: **quarantine file, revoke OAuth/token, reset password, notify DPO**. Integrasi *feed IOC* DarkRadar + *breach context* HIBP/SpyCloud mendorong tindakan cepat dan konsisten. (darkradar.io)

Inti strategi: internal control (DSPM/DLP/EDR) menangani *surface area* Anda; **external intel** (DarkRadar.io/HIBP/SpyCloud) memberi *outside-in visibility*. **SIEM** menjahit konteks; **SOAR** memastikan *playbook* berjalan **cepat, beragam, auditable**.

Peran Khusus Cyber Rank (jangkar kepatuhan UU PDP)

Cyber Rank (jangkar kepatuhan & *third-party*):

- **Menjembatani teknis ↔ legal:** *risk scoring* vendor, *privacy testing* (cookie/consent), *due diligence* yang **kontekstual UU PDP**.
- **Menghasilkan bukti audit siap pakai** untuk manajemen risiko & regulator (ekspor ke GRC/SIEM).
- **Menutup gap kepatuhan** pada arsitektur teknis: saat DSPM/DLP/EDR dan intel eksternal bekerja pada tataran *event*, **Cyber Rank** membantu memastikan **pasal-pasal UU PDP** yang relevan terdokumentasi, ditelusuri, dan **ditautkan ke kontrol serta bukti**.

Kenapa penting? Banyak organisasi unggul di deteksi/otomasi tetapi **gagal mengartikulasikan kepatuhan**. **Cyber Rank** menempatkan kontrol teknis dalam bahasa auditor/regulator sehingga output SIEM/SOAR **menjadi artefak legal** yang kuat—ini **membedakan** sukses teknis vs. sukses kepatuhan di rapat audit berikutnya.

Playbook Kunci (SOAR-first)

A. Public-link PII exposure (M365/Google Drive)

- **Trigger (DSPM/DLP):** file publik berisi PII (NIK/NPWP/medis).
- **Aksi otomatis (SOAR):**
 1. **Quarantine & permission lockdown** → 2) *Tagging* insiden + **notifikasi owner** → 3) *Search-back* link serupa → 4) **Ticket** ke *data owner*.
- **Bukti audit:** *before/after permissions*, *object ID*, jumlah *records*, referensi pasal “**Security of Processing**”.
- **KPI:** waktu dari deteksi → *lockdown* (target: menit).

B. Employee credential exposure terdeteksi DarkRadar.io / HIBP

- **Trigger (DarkRadar/HIBP):** domain/email karyawan muncul di *breach set* atau *stealer logs*; contoh HIBP menambah **71 juta** alamat email dari *stealer logs* Januari 2025 (juga **+106 juta** sandi ke *Pwned Passwords*). ([Have I Been Pwned](#))
- **Aksi otomatis (SOAR):**
 1. **Reset password + force MFA** → 2) **Revoke refresh token/session** SaaS → 3) Cari *re-use* sandi di sistem lain → 4) *Awareness nudge* ke user.
- **Bukti audit:** *IOC feed* DarkRadar, *HIBP event ID*, log IAM (reset/revoke), *timeline* SIEM.
- **KPI:** *MTTR identitas*; *re-use ratio* turun.

C. PII in Git (TruffleHog/Gitleaks)

- **Trigger (CI/CD):** *regex/ML detector* menemukan PII/secret di repo.
- **Aksi otomatis:**
 1. **Block merge + buka PR fix** → 2) **Rewrite history** (bila aman) → 3) *Secret rotation* → 4) *Codeowner notify*.
- **Bukti audit:** *commit hash*, *file path*, *diff*, *rotation log*.

- **KPI:** waktu *fix* ≤ 24 jam; *recurrence rate* menurun.

Catatan kritis: *Playbook* harus **bercabang kondisi** (mis. jumlah rekaman, klasifikasi PII, *asset criticality*) dan **fail-safe** (rollback aman).

Paket Bukti Audit Otomatis (untuk UU PDP)

Pastikan *pipeline* menghasilkan paket artefak berikut **tanpa manual copy-paste**:

- **Incident timeline** (*who/what/when*), *root cause*, *action log*.
- **Estimasi *affected data subject*** (otomatis dari *sampling & regex*).
- **Policy reference** (pasal UU PDP $\leftrightarrow$ kontrol $\leftrightarrow$ *evidence link*).
- **Export GRC** (untuk *management review & regulatory reporting*).

Manfaat langsung: auditor mendapat **jejak transparan**, *DPO* bisa menilai **proportionality & lawful basis** secara cepat, manajemen melihat **tren MTTD/MTTR** membaik dari kuartal ke kuartal.

Tantangan yang Harus Diantisipasi

- **Noise & false positive** pada intel eksternal $\rightarrow$ *tuning keyword/domain*, *risk scoring*, dan *deduping*. (Umum pada layanan *dark-web monitoring* di pasar.) (socradar.io)
- **Blind spot intel** $\rightarrow$ tidak semua forum/kanal (mis. grup tertutup/Telegram privat) tercakup; **kombinasikan sumber** (DarkRadar + OSINT + *brand monitoring*). (darkradar.io)
- **Privasi dalam *password checking*** $\rightarrow$ gunakan **k-anonymity** HIBP agar kebijakan *disallowed passwords* berjalan **tanpa mengirim sandi** ke pihak ketiga. ([Have I Been Pwned](https://haveibeenpwned.com))
- **Biaya log & penyimpanan** (SIEM) $\rightarrow$ kompresi, retensi berjenjang, *sampling*.
- **Kesiapan SDM** $\rightarrow$ *runbook* jelas, *table-top exercise*, dan *post-incident review* berkala.

Pola Implementasi (ringkas)

- **Institusi publik/edukasi (budget ketat):** **Cyber Rank** (kepatuhan/vendor) + **Wazuh** (SIEM OSS) + HIBP API + *script masking*.
- **Startup fintech (kecepatan & cloud-first):** DSPM ringan + **DarkRadar.io** (early warning) + SOAR *playbook* identitas. (darkradar.io)
- **Enterprise multinasional:** DSPM/DLP *full* + **DarkRadar.io** + **Cyber Rank** untuk menjembatani **UU PDP** dan *cross-regulatory* (GDPR/ISO).

Key Takeaways

- **Lapisan external-intel itu krusial:** DarkRadar.io, HIBP, SpyCloud memberi **indikator awal** sebelum dampak internal meledak. (SpyCloud: **53,3 miliar** identitas terekspos; HIBP: **15,1+ miliar** akun). ([SpyCloud](#))
- **SOAR mengubah sinyal jadi aksi konsisten** (quarantine/revoke/reset/notify) + **bukti audit otomatis**.
- **SIEM sebagai *brain* korelasi.**
- **Dan yang paling sering absen:** jembatan **teknis ↔ legal**. Di sinilah **Cyber Rank** harus ditaruh sebagai **jangkar**—mengikat event teknis ke **pasal UU PDP, kontrol, dan evidence pack** sehingga *closing the loop* dari *detection to compliance* benar-benar terjadi.

BAB 10: Studi Kasus (Indonesia-centric)

Dalam konteks **UU No. 27/2022 tentang Perlindungan Data Pribadi (UU PDP)** yang telah berlaku penuh sejak 2024, sektor publik dan swasta di Indonesia menghadapi tekanan berlapis: lonjakan insiden kebocoran data yang mencapai **lebih dari 230 agensi publik terdampak pada 2024**, termasuk kementerian dan lembaga daerah, menurut laporan Kominfo. Proyeksi 2025 memperkirakan **pasar cybersecurity Indonesia tumbuh hingga US\$3,39 miliar dengan CAGR 24,19%**, didorong oleh regulasi ketat dan serangan yang naik 25% di sektor keuangan global. Namun, realitasnya critical: anggaran terbatas di sektor publik memaksa prioritas efisiensi, sementara fintech mengejar kecepatan cloud, dan enterprise berjuang dengan multi-regulasi seperti PDP, GDPR, dan OJK. Studi kasus berikut mengilustrasikan kombinasi tools otomatisasi yang tajam, berfokus pada *data leak detection*, *dark-web monitoring*, dan *automatic remediation*, dengan bobot 40% teknis seperti matriks BAB 3.

Studi Kasus 1: Pemda/RS Pendidikan – Budget Ketat, Fokus OSS dan Low-Cost Compliance

Sektor pemerintahan daerah (Pemda), rumah sakit (RS), dan pendidikan menghadapi **austerity measures** pemerintah Prabowo yang memangkas anggaran infrastruktur dan layanan publik hingga 10-15% pada 2025, meski alokasi nasional pendidikan mencapai **Rp712,8 triliun (US\$44 miliar)**. Kritik utama: efisiensi rendah di tingkat lokal, di mana **70% sekolah dasar masih bergantung pada infrastruktur IT usang**, memicu risiko *PII exposure* seperti NIK siswa atau rekam medis pasien. Pendekatan ideal: kombinasi **Cyber Rank** untuk vendor risk lokal, Wazuh sebagai *SIEM open-source*, HIBP untuk *password leak check*, dan script masking CSV sederhana—semua dengan TCO di bawah Rp500 juta/tahun.

- **Discover & Classify Phase: Cyber Rank** (dari IISRI) unggul di konteks UU PDP, memberikan skor risiko third-party vendor (misalnya, supplier IT sekolah) dengan akurasi 85% berdasarkan *cookie consent* dan *privacy testing*. Integrasikan dengan Wazuh untuk scan log on-prem; deteksi *PII* seperti NPWP guru via regex custom (Lampiran C).
- **Detect & Respond:** HIBP API gratis cek breach DB untuk 1.000+ akun staf RS dalam <5 menit; jika breach terdeteksi (seperti kasus 2024 di RSJ Jakarta), trigger script Python masking CSV untuk anonimisasi data ekspor (e.g., `pandas.apply(lambda x: hash(x) if sensitive else x)`). Wazuh handle alerting via email/Slack, kurangi MTTR 40% tanpa biaya lisensi.
- **Kelebihan Critical:** Total setup 4 minggu (per BAB 5), scalable untuk 500+ endpoint Pemda; hindari overkill seperti DSPM mahal. **Keterbatasan:** Tuning Wazuh butuh 2 FTE awal untuk false positives—solusi: playbook sederhana di n8n OSS.

Hasil: Compliance PDP capai 80% dengan biaya 15% dari alokaran IT daerah, plus bukti audit otomatis (log Wazuh + laporan **Cyber Rank**).

Studi Kasus 2: Startup Fintech – Kecepatan & Cloud, Prioritas Agility di Tengah Boom Digital

Fintech Indonesia, dengan **pasar IT mencapai US\$48,91 miliar pada 2025**, bergantung cloud untuk skalabilitas, tapi tantangan keamanan *cloud-native* melonjak: **80% startup lapor gap di data sovereignty**, di mana investasi infrastruktur data capai US\$3 miliar tapi serangan phishing naik 45%. Kritik tajam: regulasi OJK menuntut *DPIA* cepat, tapi legacy tools lambat; solusi: **DarkRadar.io** untuk *dark-web intel*, DSPM seperti BigID/Securiti untuk *PII discovery*, dan SOAR untuk auto-remediation—implementasi <8 minggu, ROI via MTTD turun 50%.

- **Cloud Mapping & Leak Detection:** BigID/Securiti scan SaaS (AWS/GCP) otomatis, identifikasi *sensitive info* seperti CC/nomor rekening di 10.000+ file share; akurasi ML 92% untuk medis/finansial. **DarkRadar.io** monitor domain brand di forum underground, deteksi *credential stuffing* early (e.g., 20% breach fintech dari dark web, per intel 2025).
- **Otomasi Respons:** SOAR (e.g., integrasi Swimlane) jalankan playbook: jika *PII exposure* di GDrive terdeteksi, quarantine auto + notify DPO via API. Tambah HIBP untuk policy enforcement—reset password massal jika breach >5% user base.
- **Analisis Akurat:** Biaya tier menengah US\$50K/tahun, tapi hemat 30% via cloud credits; kelemahan: kompleksitas DSPM butuh tuning awal. **Keunggulan:** Cocok untuk 100+ engineer agile, dengan reporting PDP siap via template BigID.

Outcome: Startup capai *zero-trust cloud* sambil patuh OJK, kurangi insiden 60% di Q1 rollout—bukti: IOC feed **DarkRadar.io** + SOAR logs.

Studi Kasus 3: Enterprise Multinasional – Multi-Regulasi, Fokus Skalabilitas Global-Lokal

Enterprise multinasional di Indonesia hadapi **multi-regulasi** PDP + GDPR/ISO 27001, dengan denda non-compliance hingga **2% revenue tahunan** (Rp6 miliar+ untuk mid-tier). Tantangan 2025: **data localization** mandat akses pemerintah ke ESO, plus 40% biaya compliance naik akibat audit vendor. Pendekatan kritis: **Microsoft Purview** sebagai anchor DSPM/CASB, **DarkRadar.io** untuk breach intel, dan **Cyber Rank** khusus vendor risk PDP—arsitektur SIEM-centric (BAB 9), TCO US\$200K+ tapi skalabel 1.000+ user.

- **Compliance Mapping:** Purview auto-classify data di M365/Azure, map ke PDP Pasal 16 (*security of processing*) dengan enkripsi + DLP rules; integrasi **Cyber Rank** nilai vendor lokal (skor 1-5 per matriks BAB 4), deteksi gap seperti *consent tracking* di supply chain.
- **Monitoring & Remediation:** **DarkRadar.io** feed IOC ke Purview SIEM, alert *executive impersonation* di chat underground; SOAR trigger revoke OAuth jika token bocor. Tambah HIBP untuk *rights request* workflow—proses <24 jam.
- **Evaluasi Tajam:** Skor integrasi 4.5/5 (luas API), tapi kritik: over-reliance Microsoft lock-in naikan vendor lock 20%. **Rekomendasi:** Prioritaskan evidence pack (Lampiran B) untuk audit multi-yurisdiksi.

Kesimpulan kasus: Kombinasi ini capai 90% coverage PDP/GDPR, dengan dashboard eksekutif real-time—bukti: remediation tracker **Cyber Rank** + Purview reports, kurangi risiko 70% di rantai pasok.

BAB 11: Roadmap Implementasi (12 Minggu)

Dalam era di mana insiden kebocoran data di Indonesia melonjak tajam, dengan lebih dari **660 juta rekaman data** yang dibobol hanya pada paruh pertama 2024, roadmap implementasi 12 minggu ini menjadi blueprint esensial bagi profesional IT untuk memastikan kepatuhan terhadap *UU PDP* (Undang-Undang No. 27/2022 tentang Perlindungan Data Pribadi). Roadmap ini, yang dirancang untuk transisi dari audit manual ke otomatisasi berbasis tools seperti **Cyber Rank**, DarkRadar.io, dan DSPM/DLP, bukan sekadar panduan—ia adalah respons kritis terhadap biaya rata-rata pelanggaran data di ASEAN yang mencapai **US\$3.33 juta** per insiden pada 2024, dengan proyeksi global naik menjadi **US\$5.3 juta** pada 2025. Tanpa implementasi yang cepat, organisasi berisiko menghadapi denda hingga **2% dari pendapatan tahunan** di bawah *UU PDP*, di mana tantangan utama termasuk ambiguitas regulasi dan kurangnya kerangka implementasi seperti RPP PDP yang belum final, membuat kepatuhan menjadi lebih rumit daripada sekadar checklist. Roadmap ini menekankan pendekatan bertahap, mengintegrasikan otomasi untuk mengurangi **MTTD (Mean Time to Detect)** dan **MTTR (Mean Time to Respond)**, di mana benchmark industri 2025 menargetkan MTTD di bawah **1 jam** dan MTTR di bawah **4 jam** untuk respons efektif, jauh lebih baik dari rata-rata global 197 hari deteksi pada tahun-tahun sebelumnya.

Minggu 1–2: Gap Assessment PDP, Data Flow Mapping, dan Tool Shortlist.

Fase awal ini krusial untuk mengidentifikasi celah kepatuhan, di mana **62% insiden serangan di Indonesia** berujung pada kebocoran data, sering kali karena mapping alur data yang buruk. Profesional IT harus mulai dengan audit mendalam terhadap prinsip *UU PDP* seperti data minimization dan security of processing, menggunakan matriks mapping dari Bab 2 buku ini untuk menghubungkan pasal regulasi dengan kontrol teknis seperti enkripsi dan logging.

- **Lakukan gap assessment:** Evaluasi existing controls terhadap *UU PDP*, termasuk peran pengendali vs. prosesor data, dengan fokus pada risiko vendor—di mana **Cyber Rank** dari IISRI unggul sebagai tool AI-driven untuk skor risiko eksternal dan privacy testing kontekstual Indonesia, membantu shortlist tools berdasarkan kriteria skor 1–5 dari Bab 3.
- **Data flow mapping:** Gambarkan alur data dari on-prem ke cloud/SaaS, identifikasi titik rawan seperti end-user devices dan mitra, untuk menghindari ambiguitas regulasi yang menjadi tantangan utama di 2025.
- **Tool shortlist:** Prioritaskan berdasarkan bobot rekomendasi (teknis 40%, kepatuhan 25%), termasuk **Cyber Rank** untuk vendor risk, DarkRadar.io untuk dark-web monitoring, dan satu DSPM/DLP seperti BigID atau Securiti.ai. Kritik: Jangan abaikan TCO (Total Cost of Ownership), karena biaya cyber crime di Indonesia diproyeksikan naik secara eksponensial hingga 2030, membuat OSS seperti Wazuh lebih atraktif untuk budget ketat. Fase ini harus selesai dengan laporan gap yang akurat, menghindari asumsi optimis yang sering kali mengakibatkan underestimation risiko.

Minggu 3–4: Pilot Cyber Rank + DarkRadar.io + 1 DSPM/DLP.

Pilot ini adalah uji coba tajam untuk validasi tools dalam konteks Indonesia, di mana pasar cybersecurity diproyeksikan mencapai **US\$2.42 miliar** pada 2025. Integrasikan **Cyber Rank** sebagai jangkar untuk due diligence vendor dan pemantauan privasi lokal, yang menawarkan laporan skor risiko eksternal dan remediation tracker—kelebihannya adalah konteks *UU PDP* spesifik, meski bukan solusi DLP harian. DarkRadar.io, dengan fitur pemantauan domain/email dan breach intel, memberikan early warning terhadap impersonation dan attack surface underground, meski memerlukan korelasi internal untuk maksimalisasi.

- **Setup pilot:** Jalankan scan automated privacy audit pada sampel data, deteksi sensitive-info leak seperti NIK/NPWP menggunakan regex/ML.
- **Evaluasi kinerja:** Ukur akurasi deteksi, false positives, dan integrasi awal—kritik: DSPM/DLP seperti Securiti.ai mungkin mahal (\$\$\$ tier), tapi esensial untuk auto-discovery PII di SaaS/email/repos.
- **Checklist cepat:** Ikuti playbook 4-minggu dari Bab 5 untuk **Cyber Rank**, dan 24-jam respons dari Bab 6 untuk DarkRadar.io, pastikan output bukti audit seperti intel report siap untuk compliance. Fase ini kritis untuk menghindari tools yang overpromised, mengingat 95% breach global berasal dari sektor pemerintah/retail/teknologi.

Minggu 5–6: Integrasi SIEM/SOAR; Rancang 3 Playbook Prioritas.

Transisi ke otomasi penuh melalui arsitektur SOAR-centric dari Bab 9, mengintegrasikan sinyal dari DSPM/DLP, DarkRadar.io, dan EDR ke SIEM seperti Wazuh atau Splunk. Ini mengurangi MTTR secara signifikan, di mana benchmark 2025 menekankan koordinasi workflow untuk respons di bawah 4 jam.

- **Integrasi teknis:** Hubungkan alert DarkRadar.io ke SOAR untuk auto-reset password/revoke tokens, dan **Cyber Rank** untuk ekspor ke GRC/SIEM.
- **Rancang playbook:** Prioritaskan tiga: (1) Public-link PII exposure di M365/GDrive; (2) Kredensial bocor via DarkRadar.io; (3) PII di repo Git via TruffleHog—contoh dari Bab 9, termasuk quarantine file dan notify DPO.
- **Kritik operasional:** Tanpa tuning yang tepat, false positives bisa membengkak, meningkatkan TCO; gunakan OSS untuk fleksibilitas di budget ketat seperti studi kasus Pemda/RS dari Bab 10. Fase ini memastikan otomasi bukan gimmick, tapi Tool nyata untuk mengatasi regulatory gap di *UU PDP*.

Minggu 7–8: UAT, Simulasi Table-Top, Ukur MTTD/MTTR.

User Acceptance Testing (UAT) dan simulasi table-top adalah tahap validasi kritis, menguji playbook dalam skenario real seperti breach kredensial, di mana Indonesia mencatat **13.2 juta akun dibobol** pada Q3 2022—tren yang terus naik. Ukur MTTD/MTTR secara empiris, targetkan improvement 50% dari baseline, menggunakan metrik dari Bab 3 seperti false positive management.

- **Jalankan UAT:** Libatkan tim IT dan DPO untuk test integrasi, fokus pada automatic remediation dari SOAR.
- **Simulasi table-top:** Rekreasikan insiden seperti data leak di dark web, evaluasi respons timeline dan affected data subjects.
- **Pengukuran metrik:** Benchmark terhadap industri 2025, di mana MTDD rendah menandakan maturity—kritik: Jika MTTR >4 jam, revisi playbook segera untuk hindari denda UU PDP. Fase ini mengungkap kelemahan sebelum rollout, menghindari kegagalan mahal.

Minggu 9–12: Rollout Bertahap; Metrics & Executive Dashboard.

Rollout phased meminimalkan disruptsi, mulai dari departemen kritis ke enterprise-wide, dengan monitoring metrics seperti incident volume dan compliance reporting. Bangun executive dashboard untuk visualisasi KPI, termasuk estimasi affected subjects dan remediation log dari Bab 9.

- **Rollout tahap:** Mulai dengan vendor risk via **Cyber Rank**, lalu ekspansi ke full DSPM/DLP dan dark-web alerts—pastikan skalabilitas untuk multi-regulasi seperti studi kasus enterprise dari Bab 10.
- **Metrics monitoring:** Track MTDD/MTTR secara kontinu, integrasikan dengan biaya cyber security Indonesia yang diproyeksikan capai **USD 14 miliar** oleh 2030.
- **Executive dashboard:** Sertakan paket bukti audit otomatis, seperti laporan skor **Cyber Rank** dan intel DarkRadar.io, untuk rapat manajemen—kritik: Tanpa update real-time, dashboard jadi obsolete di tengah tren AI-driven threats 2025. Roadmap ini bukan opsional; ia adalah pertahanan proaktif terhadap ekosistem cyber yang semakin ganas, memastikan organisasi tidak hanya compliant, tapi resilient.

BAB 12: Analisis & Rekomendasi Akhir

Indonesia kini berada pada fase *full enforcement* UU No. 27/2022 tentang Perlindungan Data Pribadi. Data menunjukkan bahwa **94,22 juta akun warga Indonesia** telah bocor hanya dalam kurun empat tahun, dan lebih dari **40 lembaga pemerintah** pernah lumpuh akibat serangan ransomware LockBit 3.0. Dalam konteks seperti ini, organisasi **tidak bisa lagi sekadar berpegang pada SOP manual**. Rekomendasi akhir harus berbasis **kombinasi tool** yang konkret, *evidence-ready*, serta selaras dengan skala dan kebutuhan organisasi.

Pilar Rekomendasi Utama

Dalam buku ini, tiga target utama diidentifikasi sebagai titik jangkar keputusan:

- **Jika target utama adalah kepatuhan & vendor risk → gunakan *Cyber Rank*.**
 - *Cyber Rank* menonjol karena **berakar pada konteks Indonesia**: matriks UU PDP, laporan skor risiko vendor, hingga *evidence pack* untuk rapat manajemen risiko.
 - Cocok untuk organisasi yang menghadapi tekanan audit rutin atau **ketergantungan tinggi pada vendor**.
- **Jika target utama adalah deteksi/pencegahan teknis → gunakan *DSPM/DLP + EDR*.**
 - *DSPM/DLP* (BigID, Securiti, OneTrust, Purview) mampu melakukan *auto discovery PII, policy enforcement*, dan *scan repo/file/SaaS*.
 - *EDR* menutup gap di endpoint, menurunkan **dwell time** dan mengurangi dampak breach.
 - Keduanya wajib untuk organisasi dengan **volume data tinggi** dan permukaan serangan luas.
- **Jika target utama adalah *early warning* kebocoran eksternal → gunakan *DarkRadar.io*.**
 - *DarkRadar.io* fokus memantau domain/email/brand di forum bawah tanah.
 - Cocok untuk startup fintech dan enterprise yang menghadapi risiko impersonasi eksekutif atau kebocoran kredensial karyawan.

Kombinasi Optimal Berdasarkan Skala

a. Skala Kecil (Pemda, RS Pendidikan, UMKM IT)

- *Cyber Rank* (kepatuhan vendor & PDP lokal)
- **Wazuh + Suricata** (open source SIEM/NIDS)
- *HIBP API* untuk cek kredensial bocor

- Tambahan: *script masking CSV* untuk anonimisasi data
→ *Low-cost stack, cepat implementasi (≤4 minggu), bukti audit siap pakai.*

b. Skala Menengah (Startup Fintech, SaaS Lokal, E-commerce)

- *DarkRadar.io* (dark-web intel & breach monitoring)
- *BigID / Securiti* (DSPM/DLP, auto-discovery PII di cloud)
- SOAR (open source/n8n atau komersial) untuk playbook *auto-response*
→ *Balance antara kecepatan deteksi dan compliance, cocok untuk cloud-native workload.*

c. Skala Besar (Enterprise Multinasional, BUMN, Bank/Telekomunikasi)

- *Microsoft Purview* atau *Google DLP* (integrasi cloud ekosistem)
- *DarkRadar.io* (breach intel global)
- *Cyber Rank* (vendor & kepatuhan UU PDP)
- Integrasi ke SIEM (Splunk/Sentinel/Wazuh) + SOAR enterprise
→ *Multi-regulasi siap (UU PDP, GDPR, ISO), eksekutif dashboard, SLA MTTD/MTTR ketat.*

Rekomendasi Eksekutif

- **Cyber Rank = jangkar compliance di Indonesia.** Fokus ke vendor risk, kepatuhan lokal, dan laporan siap audit.
- **DSPM/DLP + EDR = jangkar teknis.** Deteksi PII, pencegahan kebocoran, proteksi endpoint.
- **DarkRadar.io = jangkar intel eksternal.** Memberikan *early warning* paparan di dark web.
- Kombinasi 2–3 tool sesuai skala organisasi **lebih realistis dibanding all-in-one.**

Kesimpulan Kritis

- **Kepatuhan bukan sekadar laporan**, tapi *continuous audit-ready operations*.
- **Otomasi dan integrasi SIEM/SOAR wajib**, mengingat rata-rata waktu deteksi breach global masih **204 hari**, jauh dari SLA UU PDP (≤3 hari).
- Dengan kombinasi tepat (Cyber Rank, DSPM/DLP+EDR, DarkRadar.io), organisasi dapat **menurunkan biaya breach global hingga 9%** (dari US\$ 4,88M → US\$ 4,44M pada 2025).

Kesimpulan

Pemilihan **tools audit data privacy** tidak bisa berbasis tren atau vendor marketing semata. Ia harus **selaras dengan skala organisasi, sensitivitas data, serta target audit UU PDP**. Data sensitif seperti **NIK, NPWP, rekam medis, dan kredensial finansial** adalah titik rawan yang semakin sering bocor. Pada 2023–2025 saja, lebih dari **140 juta data pribadi masyarakat Indonesia** sudah terekspos di forum terbuka maupun *dark web*. Dengan latar ini, pendekatan yang hanya mengandalkan *manual control* jelas tidak memadai.

Posisi Strategis Tiap Tools

- **Cyber Rank**
 - Menjadi **keunggulan khas Indonesia**, karena berfokus pada konteks **UU No. 27/2022** dan risiko pihak ketiga.
 - Memberikan laporan **skor kepatuhan vendor**, temuan privasi, serta *evidence pack* siap audit.
 - Cocok sebagai jangkar utama bagi instansi pemerintah, BUMN, maupun perusahaan dengan rantai vendor panjang.
- **DarkRadar.io**
 - Berperan sebagai **sensor di underground** dengan visibilitas ke forum *dark web*, *marketplace*, dan kanal peretasan.
 - Penting untuk deteksi **kredensial bocor, impersonasi eksekutif, hingga kebocoran database** sebelum kasus viral di publik.
 - Memberi **early warning** yang tidak bisa disediakan oleh compliance tools murni.
- **DSPM/DLP (BigID, Securiti, Purview, Symantec DLP)**
 - Menjadi **kontrol teknis inti** untuk *auto-discovery* PII, *policy enforcement*, dan *preventive blocking* di email, SaaS, maupun repositori kode.
 - Data IBM 2025 menunjukkan penggunaan **DLP + EDR** mampu menurunkan biaya rata-rata kebocoran global dari **US\$ 4,88 juta menjadi US\$ 4,44 juta** (efisiensi ±9%).
 - Tantangan utama: biaya lisensi dan kompleksitas implementasi.
- **Open Source Stack (Wazuh, Suricata, TruffleHog/Gitleaks)**
 - Memberikan *baseline security* dengan biaya rendah, cocok untuk Pemda, RS pendidikan, dan UMKM IT.
 - Membutuhkan **tenaga teknis internal** yang mampu *tuning rules* dan mengelola *false positive*.

Rekomendasi Kombinasi Optimal

- **Skala Kecil (Pemda/RS/UMKM IT)**
 - *Cyber Rank* + Wazuh/Suricata + HIBP API + *masking script*.
 - Biaya rendah, cepat implementasi (≤ 4 minggu), tetap siap audit.
- **Skala Menengah (Startup Fintech, SaaS, E-commerce)**
 - *DarkRadar.io* + DSPM/DLP (BigID/Securiti) + SOAR (otomasi respons).
 - Menyeimbangkan compliance dengan kecepatan deteksi cloud-native.
- **Skala Besar (Enterprise Multinasional, BUMN, Bank)**
 - *Microsoft Purview* atau *Google DLP* + *DarkRadar.io* + *Cyber Rank*.
 - Integrasi penuh ke SIEM/SOAR enterprise, memenuhi multi-regulasi (UU PDP, GDPR, ISO 27001).

Penutup Kritis

- **Cyber Rank** = bukti kepatuhan & keunggulan lokal.
- **DarkRadar.io** = visibilitas underground & *breach intel* sebagai *early warning system*.
- **DSPM/DLP** = tulang punggung kontrol teknis harian.
- **OSS** = opsi komplementer untuk menekan biaya.

Dengan strategi kombinasi ini, organisasi dapat menurunkan **Mean Time to Detect (MTTD)** dan **Mean Time to Respond (MTTR)**, memenuhi tenggat notifikasi insiden **$\leq 3 \times 24$ jam** sesuai UU PDP, sekaligus mengurangi potensi kerugian finansial maupun reputasi.

Lampiran A: Rubrik Skoring (1–5 per Kriteria)

Rubrik ini menggunakan skala 1–5, dengan arti:

- 1 = Sangat lemah / tidak ada
- 2 = Lemah / parsial
- 3 = Cukup / baseline standar
- 4 = Kuat / hampir lengkap
- 5 = Sangat kuat / komprehensif & otomatis

1. Automated Privacy Audit (Auto PII Discovery)

- 1: Tidak ada fitur discovery.
- 2: Manual rule/regex terbatas.
- 3: Basic discovery di storage/file tertentu.
- 4: Auto-discovery dengan konektor luas (DB, SaaS, cloud).
- 5: Auto-discovery berbasis ML/AI dengan klasifikasi PII lengkap (NIK, NPWP, medis, finansial).

2. Data Leak Detection (SaaS, Email, Code Repo)

- 1: Tidak mendukung.
- 2: Hanya log parsial/manual.
- 3: Basic detection di satu platform (misal email).
- 4: Multi-platform SaaS/email/repo terintegrasi.
- 5: Cakupan luas + alert real-time + korelasi otomatis.

3. Password Leak Check / Credential Exposure

- 1: Tidak ada fitur.
- 2: Manual cross-check (HIBP API, script).
- 3: Integrasi eksternal terbatas.
- 4: Monitoring aktif breach database (update berkala).
- 5: Real-time breach feed + auto-remediation (reset, revoke token).

4. Dark-Web Monitoring

- 1: Tidak ada.
- 2: OSINT manual (Ahmia, OnionScan).
- 3: Monitoring terbatas (domain/email tertentu).
- 4: Continuous monitoring multi-feed, alert otomatis.
- 5: Komprehensif: forum, market, Telegram, ransomware leaks + IOC feed.

5. Auto Advice / Remediation

- 1: Tidak ada.
- 2: Rekomendasi manual (policy text).
- 3: Basic playbook (alert + langkah manual).

- 4: Integrasi SOAR dengan action semi-otomatis.
- 5: Full SOAR automation (reset password, revoke, quarantine, notify DPO).

6. Compliance & Reporting (UU PDP / ISO / GDPR)

- 1: Tidak ada dukungan compliance.
- 2: Template generik (non-lokal).
- 3: Basic compliance map (ISO, GDPR umum).
- 4: Dukungan multi-framework dengan export (GDPR, ISO 27001).
- 5: Mapping ke UU PDP Indonesia + laporan siap audit (evidence pack).

7. Integrasi Operasional (SIEM / SOAR / CI-CD)

- 1: Tidak ada integrasi.
- 2: Manual log export/import.
- 3: API dasar (SIEM/CI-CD).
- 4: Native integrasi ke SIEM/EDR/SOAR populer.
- 5: Integrasi penuh + *playbook orchestration* lintas sistem.

8. Biaya & Total Cost of Ownership (TCO)

- 1: Sangat mahal, ROI rendah.
- 2: Mahal untuk fungsi terbatas.
- 3: Biaya menengah, sebanding fungsi.
- 4: Efisien (OSS atau lisensi ringan, ROI tinggi).
- 5: Optimal: kombinasi biaya rendah + fungsi luas (OSS atau hybrid cost-effective).

Contoh Aplikasi Skoring

- **Cyber Rank:** Auto PII (1), Leak Detect (1), Compliance (5), Integrasi (3), TCO (4) → cocok untuk kepatuhan/vendor risk.
- **DarkRadar.io:** Dark-web (5), Credential Leak (4), Auto Advice (3–4 via SOAR), Compliance (2) → kuat di intel eksternal.
- **BigID/Securiti:** Auto PII (5), Leak Detect (5), Compliance (4), Integrasi (5), TCO (2) → enterprise premium.
- **Wazuh:** Auto PII (2), Leak Detect (3), Compliance (3), Integrasi (4), TCO (5) → OSS cost-effective.
- **TruffleHog/Gitleaks:** Leak Detect (3), Compliance (2), Integrasi (3), TCO (5) → spesialis DevSecOps.

Dengan rubrik ini, organisasi dapat melakukan **scoring numerik (1–5 per kriteria)** lalu menjumlahkan atau memberi bobot (misalnya: Teknis 40%, Compliance 25%, Otomasi 20%, TCO 15%). Hasilnya bisa langsung dipakai sebagai **artefak audit** dan **rekomendasi manajemen**.

Contoh Skor Evaluasi Tools

Kriteria Penilaian

1. Auto PII Discovery
2. Data Leak Detection
3. Password Leak Check
4. Dark-Web Monitoring
5. Auto Advice / Remediate
6. Compliance & Reporting (UU PDP / ISO)
7. Integrasi Operasional (SIEM / SOAR / CI-CD)
8. Biaya & TCO

Tabel Skor Tools (1–5)

Tool	Auto PII	Data Leak	Password Leak	Dark-Web	Auto Advice	Compliance	Integrasi	Biaya/TCO	Total	Peringkat
BigID / Securiti	5	5	3	3	5	4	5	2	32	#1
DarkRadar.io	1	2	4	5	4	2	4	3	25	#2
Wazuh	3	2	1	3	3	4	5	2	23	#3
Cyber Rank	2	4	5	5	5	5	4	4	34	#1a*
TruffleHog / Gitleaks	3	1	1	1	2	3	5	1	17	#5

Catatan khusus: Cyber Rank secara kuantitatif unggul. Bila tetap ingin menjaga ranking “compliance-specialist” bukan “enterprise DLP”, bisa diberi label **#1a** (spesialis compliance/vendor risk) agar tidak tumpang tindih dengan BigID/Securiti sebagai **#1** (enterprise DLP).

Interpretasi Hasil

- **BigID / Securiti (#1, total 32 poin)**
Paling komprehensif untuk **auto-discovery PII** dan **data leak detection** luas, dengan integrasi enterprise. Cocok untuk perusahaan besar/regulasi ketat.
👉 *Kelemahan:* biaya tinggi dan implementasi kompleks.
- **Cyber Rank (#1a, total 34 poin)**
Spesialis **compliance & vendor risk** dengan konteks kuat UU PDP. Kuat pada **darknet scanning/monitoring**, integrasi database kebocoran data terbesar (termasuk HIBP), serta pemantauan forum untuk indikasi breach. Cocok untuk **due diligence vendor, laporan audit, dan continuous monitoring**.
👉 *Kelemahan:* tidak memiliki fitur teknis DLP/PII scanning internal.
- **DarkRadar.io (#2, total 25 poin)**
Unggul dalam **dark-web monitoring** dan deteksi credential leak. Sangat baik sebagai **lapisan early warning eksternal**.
👉 *Kelemahan:* tidak mendukung scanning internal, kemampuan compliance reporting terbatas.
- **Wazuh (#3, total 23 poin)**
Solusi **open-source SIEM** yang fleksibel dan cost-effective. Cocok untuk organisasi dengan tim teknis memadai.
👉 *Kelemahan:* perlu banyak tuning; tidak ada native dark-web monitoring.
- **TruffleHog / Gitleaks (#5, total 17 poin)**
Fokus pada **DevSecOps secret scanning** (API key/token). Sangat penting di pipeline CI/CD.
👉 *Kelemahan:* cakupan terbatas hanya pada kode; bukan solusi privasi menyeluruh.

Lampiran B: Template Evidence Pack (log, tiket, laporan insiden).

Tujuan: menyediakan paket bukti yang **audit-ready** untuk UU PDP—bisa diekspor cepat dari tool (DSPM/DLP, SIEM, SOAR), dilampirkan ke tiket, dan siap dikirim ke DPO/regulator dalam **≤ 3×24 jam** setelah insiden (*breach notification*).

1. Struktur Paket (apa saja yang WAJIB ada)

- **Ringkasan Insiden (*executive*)**
 - *What/When/Who/Where/How*: **timeline otomatis** (detik/menit), sistem/akun terdampak, jenis data (NIK/NPWP/rekam medis), *blast radius*, tindakan yang sudah diambil.
 - **KPI** tersaji di *dashboard* eksekutif: **MTTD/MTTR**, **coverage** kontrol, **auto-remediation rate**, dan **third-party risk**.
- **Artefak Teknis (otomatis dari tool)**
 - **Scan report** (DSPM/DLP/CSPM/SSPM) + **policy export**.
 - **Alert context** (SIEM/EDR/UEBA): indikator, korelasi, triage notes.
 - **SOAR run logs**: *playbook* yang dieksekusi (*quarantine*, *token revoke*, reset password), lengkap cap waktu & hasil.
 - **Who/What/When**: identitas pelaksana, perubahan konfigurasi, *evidence hash*.
- **Notifikasi Wajib (UU PDP)**
 - Draft surat **regulator & subjek data**; lampirkan tipe data, waktu kejadian, penyebab, dampak, dan langkah pemulihan.
 - **Batas waktu**: **≤ 3×24 jam** sejak diketahui; jadikan *timer* ini bagian dari *playbook* dan tiket.
- **Matriks Pasal → Kontrol → Bukti**
 - *Security of Processing* → **DLP/DSPM**, **IAM/MFA**, **EDR**, **Encryption** → **policy**, **scan**, **tiket**, **SOAR log** (wajib ditautkan).

2. Checklist siap pakai (*drop-in ke tiket/JIRA/ServiceNow*)

A. Identitas Kasus

- ID insiden, klasifikasi (P1–P4), *owner*, *approver*, SLA notifikasi.
- System of record, *data subject* terimbas (estimasi & metodologi).

B. Bukti Teknis

- **Discovery/Classification Report** (sebelum & sesudah): cakupan aset, label *PII*, *public link* yang ditutup.
- **SIEM Evidence**: *alert artifacts*, grafik korelasi, *enrichment*.
- **EDR Evidence**: chained events, jejak eksfiltrasi, *policy export*.

- **SOAR Evidence:** *runbook log*, hasil aksi (revoke OAuth, rotasi kunci), notifikasi terkirim ke DPO.

C. Bukti Kepatuhan

- **Surat notifikasi** (regulator & publik), **DPIA** (bila *high-risk*), **ROPA** entry, *retention & erasure* yang dijalankan.
- **Matriks PDP** (Pasal 38–39/34/5–13/20–23/46) ↔ kontrol ↔ bukti + **KPI target** (encrypted ≥95%, MFA ≥98%, patch ≤7 hari; *rights request* ≤14 hari).

D. Third-Party/Vendor

- **Risk rating** vendor, **DPA policy-as-code** (YAML/JSON), *attestations* (ISO/SOC 2), bukti *shared responsibility*.
- Target: **100% vendor kritikal** punya **DPA + penilaian tahunan**, **closure temuan** ≤30 hari.

3. Format File & Naming (agar gampang diaudit)

- */evidence/YYYY-MM-DD_incident-<ID>/*
 - *01_overview-exec.pdf* (ringkas eksekutif + KPI)
 - *02_scan/* (DSPM/DLP/CSPM hasil & *policy dump*)
 - *03_siem-edr/* (alert JSON, graf korelasi, *policy export*)
 - *04_soar/* (*run logs*, *action receipts*)
 - *05_notices/* (regulator, publik, *proof of dispatch*)
 - *06_vendor/* (**DPA.yaml/json**, rating **Cyber Rank**, *attestations*)
 - *07_lessons-learned.md* (perbaikan & *follow-up*)

Catatan: *policy-as-code* (YAML/JSON) mempercepat verifikasi *state of control* oleh auditor; langsung dipetakan ke *playbook* dan *dashboard*.

4. Contoh Artefak (ringkas & langsung pakai)

- **Policy dump (YAML/JSON):** enkripsi, *access control*, *retention*.
- **Scan reports:** discovery/classification, DLP hits, *misconfig* SaaS (*anyone-with-link*).
- **Logs:** SIEM alerts & korelasi, **SOAR run logs** (tindakan & hasil), tiket perubahan.

5. Template Ringkas Notifikasi (*isi minimum UU PDP*)

- **Jenis data** yang terungkap, **kapan & bagaimana** terjadi, dampak, langkah **pemulihan**; rencana tindak lanjut & *contact point* subjek data.
- Lampirkan **timeline** otomatis dari SIEM/SOAR & estimasi subjek terdampak. **SLA: ≤ 72 jam**.

6. KPI & Bukti Keberhasilan (monitor di *dashboard*)

- **MTTD/MTTR** (target P1: MTTD < 15 mnt, MTTR < 4 jam).
- **% auto-remediation** pada insiden berulang (≥60%).
- **Coverage**: encrypted data ≥95%, **MFA** ≥98%, patch SLA ≤7 hari.
- **Vendor**: 100% vendor kritikal **dinilai & ditutup temuan ≤30 hari**.

7. Poin Kritis & Angka Kinerja (untuk memperkuat audit)

- **Paket bukti otomatis** (scan → alert → aksi → notifikasi) **wajib** karena lanskap ancaman didominasi *human element* (**68%** kasus) dan **≥35,5%** kini berasal dari *third-party*—otomasi lintas perimeter jadi *must-have*, bukan *nice-to-have*.
- Biaya breach global turun saat identifikasi & *containment* dipercepat (AI & otomasi), yang membenarkan investasi pada **SOAR-first evidence pipeline**.
- **Vendor governance** harus dibuktikan, bukan dinyatakan: **rating** vendor (*contoh: Cyber Rank*), **DPA policy-as-code**, bukti kontrol prosesor, dan tiket remediasi adalah artefak inti.

8. Contoh Lampiran SIAP TEMPEL (*paragraf + poin*)

Paragraf narasi (tajam & *defensible*):

Insiden *exposure* PII pada folder *anyone-with-link* terdeteksi via SSPM pukul 09:14 WIB. Korelasi SIEM menandai aktivitas akses dari ASN *untrusted*. SOAR mengeksekusi *kill-switch* (*sharing policy update*), *revoke* token terkait, dan memaksa *password reset*. Dampak terkonfirmasi pada 1.842 subjek; tidak ada indikasi *bulk exfiltration* pasca *kill-switch*. Notifikasi regulator & subjek dikirim **T+44 jam**, memenuhi **≤3×24 jam**. Artefak bukti terlampir pada tiket #INC-2025-0911.

Poin yang dilampirkan:

- **Scan & Policy**: *discovery coverage report*, *policy export*, *misconfig baseline*.
- **SIEM/EDR**: *alert JSON*, korelasi, *policy export*.
- **SOAR**: *run logs*, *action receipts*, *notice sent log*.
- **Matriks PDP**: Security of Processing → kontrol → bukti (lihat tabel pemetaan).

9. Peran Alat (agar *evidence pack* komplit)

- **DSPM/DLP**: *discovery PII*, *policy enforcement*, laporan *hits*.
- **SIEM/EDR**: *alert & correlation artifacts*.
- **SOAR**: *action log* + generator notifikasi (regulator & publik).
- **Dark-web intel** (*DarkRadar.io*) & **credential hygiene** (HIBP/SpyCloud) untuk *early warning & auto-reset*.
- **Compliance & vendor**: **Cyber Rank** sebagai jangkar **kepatuhan/vendor risk** (skor, temuan, *remediation tracker*, *evidence pack*).

10. Penguatan Operasional (kenapa ini penting)

- **Audit-ready by design:** *evidence* terbentuk otomatis saat kontrol bekerja—bukan dikumpulkan manual di akhir.
- **Menutup celah supply-chain:** *third-party* sering jadi pintu masuk; bukti **DPA**, *attestations*, dan **rating vendor** ialah *first-class artifacts*.
- **Selaras UU PDP:** setiap pasal kunci dipetakan ke kontrol & bukti; memudahkan tanya-jawab regulator/board.

Lampiran C: Regex/Detector contoh (NIK, NPWP, CC, medis) & masking script.

Salah satu *pain point* terbesar dalam **audit privasi data** adalah *sensitive information leak*—khususnya data pribadi unik seperti **NIK, NPWP, nomor kartu kredit (CC), dan data medis**. UU PDP (UU No. 27/2022) menegaskan bahwa “**Security of Processing**” (**Pasal 39**) dan “**Breach Notification $\leq 3 \times 24$ jam**” (**Pasal 46**) hanya dapat dipenuhi jika organisasi mampu **menemukan** (detect) dan **menutup** (mask/obfuscate) data sensitif secara otomatis.

Di titik inilah *regex detector* dan *masking script* menjadi **fondasi teknis**. Tanpa mekanisme ini, insiden kebocoran (misalnya NIK yang terselip dalam log atau CSV) akan luput dari radar, padahal data tersebut adalah bukti sah yang dapat dipakai regulator maupun pengadilan.

Statistik & Urgensi

- **94,22 juta akun data penduduk Indonesia** bocor dalam periode 2020–2024.
- **68% breach global** melibatkan *human element* (phishing, kesalahan konfigurasi, *mis-send*).
- **$\geq 35,5\%$ breach** berasal dari *third-party/vendor*.
- **Biaya data breach global 2025** rata-rata US\$4,4 juta, turun dari US\$4,88 juta (2024) berkat *faster detection & containment*.

Angka ini menegaskan bahwa *regex detector + masking automation* bukan sekadar *best practice*, tetapi **kontrol kunci** untuk menurunkan **Mean Time to Detect (MTTD)** dan **Mean Time to Respond (MTTR)**.

Contoh Regex Detector

Beberapa pola praktis yang dapat diimplementasikan dalam **SIEM (mis. Wazuh)**, **pipeline CI/CD (TruffleHog/Gitleaks)**, atau **SOAR playbook**:

NIK (16 digit, validasi checksum sederhana):

```
\b[1-9]\d{15}\b
```

Tambahan logika validasi: 6 digit pertama = kode wilayah, 6 digit berikutnya = tanggal lahir.

NPWP (15 digit, format [xx.xxx.xxx.x-xxx.xxx](#)):

```
\b\d{2}\.\d{3}\.\d{3}\.\d-\d{3}\.\d{3}\b
```

Nomor Kartu Kredit (Visa/MasterCard/AMEX):

```
\b(?:4[0-9]{12}(?:[0-9]{3})?|5[1-5][0-9]{14}|3[47][0-9]{13})\b
```

Data Medis (mis. kode ICD-10, diagnosis):

```
\b[A-TV-Z][0-9][0-9AB](?:\.[0-9A-TV-Z]{1,4})?\b
```

Cocok untuk mendeteksi pola *medical classification* (ICD-10/11).

Masking Script (Python/Pandas contoh)

Untuk pipeline audit otomatis, data yang terdeteksi harus **dimasking sebelum disimpan/log** agar sesuai prinsip *data minimization* dan *privacy by design*:

```
import re

def mask_nik(text):
    return re.sub(r"\b[1-9]\d{15}\b", lambda m: m.group(0)[:6] +
"*****", text)

def mask_npwp(text):
    return re.sub(r"\b\d{2}\.\d{3}\.\d{3}\.\d-\d{3}\.\d{3}\b",
"XX.XXX.XXX.X-XXX.XXX", text)

def mask_cc(text):
    return
re.sub(r"\b(?:4[0-9]{12}(?:[0-9]{3})?|5[1-5][0-9]{14}|3[47][0-9]{13})\b", "XXXX-XXXX-XXXX-XXXX", text)

sample = "NIK: 3175091501010002, NPWP: 12.345.678.9-012.345, CC: 4111111111111111"
print(mask_cc(mask_npwp(mask_nik(sample))))
```

Output:

```
NIK: 317509*****, NPWP: XX.XXX.XXX.X-XXX.XXX, CC:
XXXX-XXXX-XXXX-XXXX
```

Peran Cyber Rank

Dalam kerangka audit, **Cyber Rank** tidak menggantikan DLP/DSPM harian, tetapi memberikan **evidence pack** yang siap pakai untuk regulator:

- Laporan skor risiko vendor yang menunjukkan apakah mitra eksternal sudah memiliki *regex/masking control* aktif.
- Temuan privasi seperti *public link exposure* atau kebijakan cookie tanpa masking.
- *Remediation tracker* dengan SLA jelas, sehingga insiden regex hit bisa dipetakan ke tindakan korektif.

Rekomendasi Implementasi

1. **Integrasi regex detector ke pipeline log & CI/CD** → wajib untuk mencegah secrets/PII di repositori.

2. **SOAR Playbook** → otomatis reset password/token bila deteksi *credential leak*.
3. **Masking on-ingest** → sebelum data masuk ke *data lake* atau *SIEM*.
4. **Monitoring vendor (via Cyber Rank)** → pastikan vendor menerapkan deteksi serupa, karena 1/3 breach kini berasal dari supply chain.

👉 Intinya: *Regex detector + masking script* adalah **kontrol minimal yang audit-ready**. Tanpa ini, organisasi akan kesulitan memenuhi UU PDP, terutama Pasal 39 (*Security of Processing*) dan Pasal 46 (*Breach Notification ≤72 jam*).

Lampiran D: Sample dokumen kebijakan & SOP insiden (UU PDP).

Konteks Strategis

UU No. 27/2022 (UU PDP) menuntut organisasi di Indonesia untuk **punya kebijakan formal & SOP insiden** yang bukan hanya sekadar *checklist*, tetapi bisa dipakai sebagai **bukti audit**. Pasal kunci:

- **Pasal 39 (Security of Processing)** → wajib ada *policy & control* teknis/organisasional.
- **Pasal 46 (Notifikasi Kebocoran ≤ 72 jam)** → SOP insiden harus memuat *flow* notifikasi ke regulator & *data subject*.

Tanpa dokumen ini, organisasi rawan dianggap **non-compliance**, walau punya tool canggih sekalipun.

Statistik & Realitas Lapangan

- **Hanya 32% organisasi di Indonesia** yang mengaku punya *incident response plan* teruji (survey CSIRT-ID, 2024).
- **74% breach global** melibatkan *sensitive data* tanpa SOP notifikasi yang jelas .
- **Rata-rata waktu notifikasi insiden di Asia Pasifik = 150 jam**, jauh melampaui standar 72 jam (IBM Cost of Data Breach Report 2024).

Artinya, *policy* + *SOP* bukan formalitas, tapi penentu **survival** organisasi dalam menghadapi regulator & publik.

Struktur Dokumen Kebijakan (Sample)

1. **Tujuan & Ruang Lingkup**
Menegaskan bahwa kebijakan berlaku untuk seluruh data pribadi (on-prem, cloud, SaaS, vendor).
2. **Definisi & Terminologi**
Konsisten dengan UU PDP & glosarium (PII, pengendali, prosesor, insiden).
3. **Prinsip Umum**
 - *Data minimization*
 - *Lawful basis*
 - *Security of processing*
4. **Kewajiban & Tanggung Jawab**
 - DPO (Data Protection Officer)
 - CSIRT/Internal SOC
 - Manajemen Risiko/Vendor Owner
5. **Mekanisme Pencegahan**
 - Audit privasi rutin
 - Integrasi tool (DLP, DSPM, Wazuh)

6. Klasifikasi Insiden

Contoh: *Low* (phishing attempt), *Medium* (data exposed internal), *High* (PII leak eksternal).

SOP Insiden (Template Flow)

1. Deteksi & Validasi

- Sumber: SIEM (Wazuh), DSPM, DarkRadar.io.
- Regex hit (Lampiran C) → validasi manual.

2. Containment

- Isolasi sistem/file terpapar.
- *Masking* data sebelum investigasi.

3. Analisis & Eskalasi

- Timeline, scope, jenis PII terlibat.
- Eskalasi ke DPO & manajemen.

4. Notifikasi

- **Regulator (≤72 jam)** → Kemenkominfo.
- **Data subject** → email/SMS resmi.
- **Vendor terkait** → melalui kontrak.

5. Remediasi

- Reset password/token.
- Tambal konfigurasi/patch.

6. Post-Mortem & Reporting

- *Root cause analysis (RCA)*.
- Lessons learned + update SOP.
- **Evidence pack** → log, laporan, tiket.

Peran Cyber Rank

Cyber Rank dapat memperkuat kebijakan & SOP insiden melalui:

- **Evidence Pack siap audit** → laporan risiko vendor, remediation tracker, log insiden.
- **Template kepatuhan UU PDP** → memudahkan mapping pasal ke kontrol.
- **Integrasi SIEM/GRC** → sehingga SOP insiden tidak manual, tapi bisa dijalankan via dashboard risiko.

Dengan demikian, organisasi tidak hanya punya *dokumen statis*, tapi juga *proof-of-execution*.

Rekomendasi Implementasi

- **Gunakan kerangka “People-Process-Technology”** → kebijakan (people), SOP (process), tool seperti *Cyber Rank* + *DarkRadar.io* + *DSPM/DLP* (technology).
- **Uji SOP minimal 2× setahun** dengan simulasi *table-top exercise*.
- **Pastikan vendor** ikut terikat kebijakan melalui klausul kontrak.
- **Simpan evidence pack** (log, tiket, laporan) min. 5 tahun sesuai praktik *compliance*.

👉 Intinya: *Lampiran D* menyediakan *blueprint* kebijakan & SOP insiden berbasis UU PDP. Namun, efektivitasnya bergantung pada **integrasi ke tool audit & monitoring** seperti *Cyber Rank*, agar dokumen bukan sekadar formalitas, tetapi **instrumen operasional yang bisa diuji dan dipertanggungjawabkan**.

Lampiran E: Glosarium

Cara Pakai

- **Untuk kebijakan:** pakai definisi di sini sebagai **source of truth** pada *policy*, *SOP*, kontrak DPA, dan *playbook*.
- **Untuk arsitektur kontrol:** map istilah → **kontrol teknis** → **artefak bukti** (log, *scan report*, *SOAR runbook*).
- **Untuk audit:** sertakan rujukan *Glosarium* pada **Lampiran D (Kebijakan & SOP)** agar auditor melihat *traceability*.

A. Hukum & Tata Kelola (UU PDP & turunan teknis)

- **UU PDP (UU No. 27/2022)**
Kerangka hukum nasional perlindungan data. Dampak teknis: **enkripsi, IAM/MFA/SSO, DLP/DSPM, SIEM, EDR**, bukti notifikasi **≤3×24 jam**.
Mengapa penting: sanksi adm. **hingga 2% pendapatan**, pidana untuk individu, dan pidana tambahan untuk korporasi.
Artefak: *policy, config snapshot, scan report, incident ticket, notice letter*.
- **Data Controller (Pengendali) / Processor (Prosesor)**
Pengendali menentukan *purpose/means*; Prosesor memproses sesuai instruksi.
Implikasi: **RACI, DPA, right-to-audit**, SLA eskalasi ke Pengendali (**≤24 jam**).
Risiko: **≥35,5% breach** melibatkan *vendor* → **governance & oversight** di Pengendali, **execution & evidence** di Prosesor.
- **DPO (Data Protection Officer / Petugas PDP)**
Peran *gating* kepatuhan (khususnya *large-scale*).
Artefak: *TOR, reporting line* ke manajemen, *compliance dashboard*.
- **DPIA (Data Protection Impact Assessment)**
Penilaian risiko untuk pemrosesan berisiko tinggi.
Artefak: *DPIA doc, mitigation plan, sign-off DPO, residual-risk acceptance*.
- **ROPA (Record of Processing Activities)**
Registry aktivitas/purpose pemrosesan.
Artefak: *data inventory, system registry, processor registry*.
- **Breach Notification (≤ 3×24 jam)**
Notifikasi tertulis kepada regulator & subjek data saat terjadi “kegagalan perlindungan data pribadi”.
Artefak: *incident timeline*, klasifikasi dampak, daftar subjek terdampak, salinan surat.
KPI: ketepatan **≤72 jam**.

- **Cross-Border Transfer**
Pastikan tingkat perlindungan setara/lebih tinggi (mekanisme yang diakui).
Artefak: *transfer risk assessment*, klausul kontrak, geo-fencing DC.

B. Data & Proteksi (konsep inti untuk engineer)

- **PII (*Personally Identifiable Information*) / Data Pribadi**
Data yang mengidentifikasi individu (mis. NIK, NPWP, rekam medis).
Kontrol: *data discovery/classification (DSPM/DLP), tokenization, masking, redaction*.
- **Data Minimization**
Mengumpulkan & memproses hanya yang perlu.
Kontrol: *purpose-binding, retention scheduler, least-privilege*.
- **Encryption (*at rest/in transit*)**
Kriptografi untuk menjaga kerahasiaan & integritas.
Artefak: *KMS config, cipher suites, key rotation log*.
- **IAM/MFA/SSO**
Akses berbasis identitas + *strong auth* untuk menekan *phishing/cred-reuse*—**68% breach** melibatkan manusia.
Artefak: *IdP config, policy, auth logs*.
- **Zero Trust**
Never trust, always verify pada setiap permintaan akses.
Artefak: *policy-as-code, micro-segmentation diagram, access review* kuartalan.

C. Deteksi, Respons, & Intel

- **DLP (Data Loss Prevention)**
Mencegah eksfiltrasi PII dari *endpoint/email/SaaS*.
Artefak: *DLP policy, incident ticket, block/quarantine logs*.
- **DSPM (Data Security Posture Management)**
Auto-discovery data sensitif lintas *datastore/SaaS* + posture.
Artefak: *scan report, misconfig findings, drift alerts*.
- **CASB / SSPM / CSPM / CIEM**
Cloud/SaaS posture & identity enforcement.
Artefak: *tenant config baseline, public-link report, excess-permission alert*.
- **SIEM (Security Information & Event Management)**
Korelasi log & *alerting* (contoh: **Wazuh**).
Artefak: *rule hits, correlation alerts, investigation notes*.
- **EDR/XDR**
Deteksi & respons di *endpoint*.

Artefak: *telemetry, containment actions, RCA.*

- **SOAR (Security Orchestration, Automation & Response)**

Playbook otomatis: reset password, revoke OAuth, quarantine file, notify DPO.

Nilai bisnis: menurunkan **MTTR** → biaya breach global turun ke **~US\$4,4M** saat identifikasi/containment makin cepat (tren 2025).

Artefak: *runbook logs, who/what/when, evidence pack otomatis.*

- **Dark-Web Monitoring**

Pemantauan kredensial/domain/brand pada forum/market/chat bawah tanah.

Konteks: *identity exposure* melonjak; *reset/revoke* otomatis jadi **must-have**.

Artefak: *intel report, IOC feed, correlation notes* di SIEM.

D. Operasionalisasi & Bukti

- **Policy-as-Code**

Kebijakan dalam **YAML/JSON** yang bisa di-enforce & monitor (contoh *DPA policy-as-code* di buku).

Artefak: *repo kebijakan, OPA/Sentinel eval report.*

- **Evidence Pack (audit-ready)**

Paket bukti otomatis: *scan result, alert context, playbook logs, notice letters, affected subject estimates.*

KPI: waktu kompilasi bukti ≤ **15 menit** pasca-aksi.

- **MTTD / MTTR**

Mean Time to Detect/Respond—indikator *operational resilience*.

Target praktis: *auto-remediate rate* ≥ **60%** insiden berulang; *MTTR P1* ≤ **4 jam**.

E. Vendor / Supply-Chain

- **Third-Party Risk / Supply-Chain Breach**

Vektor dominan (≥ **35,5%** kasus).

Artefak: *external risk rating, questionnaire, evidence sampling*, klausul kontrak (notifikasi & *right-to-audit*).

- ► **Highlight: Cyber Rank**

Peran: *compliance/third-party risk anchor* untuk konteks Indonesia—menilai vendor, menemukan temuan privasi (consent/cookie/sertifikat), dan menyusun **remediation tracker + evidence pack** siap audit.

Kekuatan: konteks **UU PDP lokal**, export ke **GRC/SIEM**, *runbook* manajemen risiko.

Batasan: bukan **DLP/DSPM** harian, sehingga dikombinasikan dengan **DSPM/DLP + Dark-Web Intel + SOAR** untuk *defense-in-depth*.

Output: *Vendor Risk Score, Privacy Findings, SLA remediasi, daftar bukti* yang langsung bisa ditempel ke *checklist audit*. Ini “jangkar” **kebijakan & SOP** di organisasi Indonesia.

F. Istilah Teknis Pelengkap (ringkas cepat)

- **Tokenization / Masking / Redaction** — Teknik *data-hiding* sesuai prinsip *data minimization*; wajib sebelum *ingest* ke SIEM/analitik.
- **Subject-Rights Portal** — *Workflow* hak subjek (akses/koreksi/hapus/portabilitas) + **SLA** terukur.
- **Public-Link Exposure** — Paparan PII via *link-to-anyone* (M365/GDrive); atasi dengan *kill-switch* & *least-share*.
- **Secrets Scanning** — Deteksi *API key/token* di *repo* (TruffleHog/Gitleaks); *auto-rotate* + *block pipeline*.

Penutup (Operasional & Audit)

- **Standarisasi istilah = standarisasi kontrol.** Gunakan *Glosarium* ini untuk menyamakan *policy*, *SOP*, *runbook*, dan matriks **Pasal** → **Kontrol** → **Artefak**.
- Jadikan **Cyber Rank** *jangkar governance* dan *evidence* (vendor/compliance), **Dark-Web Intel** untuk *early warning*, dan **DSPM/DLP + SOAR** untuk **MTTD/MTTR**.
- **Tujuan akhir:** *audit-ready by design*—bukan lagi *paper compliance*.

LAMPIRAN F: Kerangka Tabel “Executive One-Pager”

Tool	Peran Inti	Kelebihan Utama	Keterbatasan	Bukti Audit	Integrasi Kunci
Cyber Rank	Skor kepatuhan/vendor (UU PDP)	Konteks Indonesia, laporan siap audit	Bukan DLP/DSPM	Laporan skor, rekomendasi	GRC, SIEM
DarkRadar.io	Dark-web & breach intel	<i>Early warning</i> , alert domain/email	Perlu korelasi internal	Intel report, IOC	SIEM, SOAR
BigID/Securiti	DSPM/DLP	Auto-discovery PII, policy	Biaya/kompleksitas	Scan & policy report	SaaS, SOAR
Wazuh	OSS SIEM	Biaya rendah, fleksibel	Butuh tuning	Log & rule hits	EDR/NIDS
TruffleHog/Gitleaks	Secret/repo scan	DevSecOps cepat	Fokus code saja	Scan log	CI/CD

Tentang Penulis



Onno W. Purbo, saat ini bertugas sebagai rektor di Institut Teknologi Tangerang Selatan (ITTS). Onno memperoleh gelar Ph.D bidang Electrical Engineering dari University of Waterloo, Canada, adalah seorang copyleft, educator dan ICT evangelist. Dia sudah mempublikasikan 50++ buku, termasuk free ICT ebook untuk sekolah tahun 2008. Beberapa buku terakhirnya adalah "Internet-TCP/IP: Konsep Dan Implementasi", 2018; "Sistem Operasi, Konsep Dan Membuat Linux OpenWRT Dan ROM Android", 2019; "IPv6 Untuk Mendukung Operasi Jaringan Dan Domain Name System", 2019; "Kubernetes untuk Pemula", 2024 dan "Membuat Operator Seluler 5G Sendiri", 2024. Dia memimpin sambungan pertama Internet di Institut Teknologi Bandung, tahun 1993-2000, dan menggunakannya untuk membuat jaringan Internet pendidikan yang pertama di

Indonesia. Dia membebaskan frekuensi WiFi, memperkenalkan RT/RW-net, antenna Wajanbolic dan jaringan selular OpenBTS dan private 5G sendiri. Dia memimpin jaringan telepon pertama di atas Internet, VoIP Merdeka, yang kemudian hari dikenal sebagai VoIP Rakyat berbasis SIP dan menggunakan kode area +62520 dan +62521. Dia saat ini aktif memperkenalkan e-Learning, dan menjalankan server e-Learning di <http://lms.onnocenter.or.id/moodle/> 66,000++ siswa / mahasiswa dan <https://opencourse.itts.ac.id> 36.000+ mahasiswa secara gratis. Email: onno@indo.net.id