Journal of Applied Informatics and Computing (JAIC)
Vol.10, No.4, August 2026, pp. 3808~3814
e-ISSN: 2548-6861

Mapping Compliance–Maturity Gaps in EdTech Personal Data Security: Integrating the PDP Law and KAMI Index 5.0

Ocha Oktafia [1*], Nelmiawati [2*], Putri Hening Graha [3], Kessy Dealova[4*]**
[*]Cyber Security Engineering, Politeknik Negeri Batam
[**]Public Policy, National University of Singapore
oktaaochaa1101@gmail.com [1], mia@polibatam.ac.id [2], putrihening@u.nus.edu [3], kessydealova30@gmail.com [4]

Article Info

Article history:

Received 2026-06-25
Revised 2026-07-25
Accepted 2026-08-12

Keyword:

EdTech,
ISO/IEC 27002:2022,
KAMI 5.0 Index,
PDP Law

ABSTRACT

The rapid post-pandemic growth of Educational Technology (EdTech) platforms in Indonesia is not always accompanied by personal data security readiness, despite the high compliance demands mandated by Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Previous studies utilizing the KAMI Index generally assessed technical maturity separately from legal frameworks, leaving a gap in understanding how regulatory compliance correlates with technical maturity within a single entity. This study aims to evaluate the information security maturity level and legal compliance of PT XYZ's EdTech platform, while simultaneously mapping the connection between the PDP Law requirements and the assessment areas of KAMI Index 5.0. This research employs a qualitative case study approach. Data were collected through questionnaires based on the KAMI Index 5.0 instrument and PDP Law articles, completed by three key respondents—the CEO, CTO, and VP of Information Security—and subsequently validated through interviews and verification of supporting documents. The results reveal a significant gap: procedural compliance with the PDP Law is relatively high (28 out of 36 articles fully implemented), yet the KAMI Index maturity level falls into the "Inadequate" (*Tidak Layak*) category with a final score of 222. The system is notably weak in risk management and personal data protection areas (Level I+). These findings emphasize that procedural compliance does not equate to holistic security maturity. This research contributes by providing a legal-technical gap mapping alongside recommendations based on ISO/IEC 27002:2022, which can be adopted by other EdTech organizations.

I. PENDAHULUAN

Pandemi COVID-19 telah mempercepat adopsi teknologi digital, khususnya di sektor pendidikan [1]. Data World Bank menunjukkan pengguna aktif platform EdTech meningkat 200% pada Maret 2020, dan di Indonesia lebih dari 210 startup EdTech muncul pada tahun 2021, menandai perkembangan pesat industri ini [3]. Seiring pertumbuhan tersebut, pengelolaan dan pelindungan data pribadi pengguna menjadi sangat penting. Badan Siber dan Sandi Negara (BSSN) mencatat 347 insiden siber dengan kebocoran data sebagai kategori tertinggi, sementara penelusuran pada *darknet* menemukan 1.674.185 temuan data exposure yang berdampak pada 429 stakeholders di Indonesia [2]. Urgensi ini bukan sekadar risiko teoretis, platform PT XYZ sendiri sempat mengalami percobaan serangan siber berupa backlink dan backshell pada tahap uji coba beta, yang mengindikasikan bahwa ancaman terhadap keamanan data pribadi telah dihadapi langsung meski platform masih berada pada tahap pengembangan awal. Temuan-temuan ini menunjukkan bahwa percepatan digitalisasi belum diiringi tingkat keamanan informasi yang memadai [4].

Platform XYZ merupakan sistem pembelajaran daring berbasis Learning Management System (LMS) yang menyediakan materi pendidikan di bidang teknologi dan desain, serta memungkinkan pengguna mengakses, mengelola, dan menyelesaikan pembelajaran secara mandiri. Privasi dan pelindungan data menjadi tantangan utama dalam

integrasi *learning analytics* pada *platform* LMS. Setiap tahap siklus learning analytics menyimpan risiko pelanggaran data pribadi, terutama ketika tidak disertai kontrol keamanan yang memadai, sebagaimana ditemukan Liu dan Khalil [5]. Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), data pribadi mencakup informasi yang dapat mengidentifikasi individu secara langsung maupun tidak langsung, dan terbagi menjadi data pribadi umum serta data pribadi spesifik, yang pengumpulannya wajib disertai persetujuan pemilik data [7], [8], [9]. Platform XYZ memproses keduanya: data umum seperti nama, surel, dan foto profil untuk login dan pengelolaan akun, serta data spesifik seperti informasi rekening dan transaksi pada fitur pembayaran dan penarikan dana. Kemudahan layanan digital ini memunculkan tantangan baru yang menuntut regulasi guna menjamin pelindungan data pribadi pengguna [6].

Untuk itu, penelitian ini mengevaluasi *platform EdTech* menggunakan Indeks KAMI dan UU PDP. Indeks Keamanan Informasi (Indeks KAMI) adalah alat evaluasi yang dikembangkan BSSN untuk menilai kesiapan instansi dalam mengelola dan melindungi informasi yang dikelola [10]. Sementara itu, UU PDP yang disahkan melalui Undang-Undang Nomor 27 Tahun 2022 bertujuan melindungi hak privasi individu dengan mengatur pengumpulan, penggunaan, dan pengelolaan data pribadi, serta berlaku bagi semua entitas yang mengelola data pribadi, baik secara elektronik maupun non-elektronik [9].

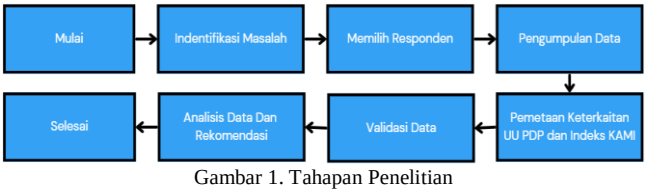
Beberapa penelitian terdahulu menunjukkan adanya kesenjangan antara kepatuhan prosedural dan kesiapan teknis dalam pengelolaan keamanan informasi. Wasilah dkk. dan Azmi dkk. menemukan bahwa instansi pendidikan dan pemerintah daerah masih berada pada tingkat kematangan rendah, terutama dalam pengelolaan risiko dan aset informasi, meskipun ketergantungan terhadap sistem elektronik cukup tinggi [11], [12]. Temuan serupa disampaikan Jenny dkk. dan Khamil dkk., di mana hanya sebagian area memenuhi standar ISO/IEC 27001, sementara area lain masih memerlukan penguatan kebijakan dan pengawasan internal [13], [14]. Rizkillah menyoroti lemahnya pelindungan data pribadi di sebuah perguruan tinggi, yang mana hanya satu dari enam kategori mencapai tingkat kematangan II [16]. Jelita dkk. pada PT Kano Teknologi Utama mencatat hanya area tata kelola dan teknologi informasi yang memenuhi standar, sementara area lainnya masih pada tingkat dasar [17], sedangkan Maryanto dkk. menemukan perusahaan rintisan berbasis teknologi umumnya masih berada pada tingkat kematangan awal (I–I+) [18]. Studi Rahayu dkk. dan Saputra dkk. di dua Diskominfo daerah mengungkap skor kematangan yang bervariasi antara I+ hingga III+, dengan kelemahan mencolok pada SOP internal, pengelolaan risiko, dan pelindungan data pribadi [19], [20]. Sebagai pembanding, Yuliani dkk. menunjukkan bahwa organisasi yang telah mapan secara tata kelola dapat mencapai tingkat kematangan tinggi [15], sehingga kesenjangan yang berulang pada mayoritas studi tampak berkaitan erat dengan belum matangnya perencanaan keamanan pada organisasi tahap awal. Secara keseluruhan, studi-studi tersebut memberikan gambaran kematangan teknis, namun umumnya menilai keamanan informasi sebagai persoalan teknis semata dan belum menautkannya secara eksplisit dengan kewajiban hukum pelindungan data pribadi.

Kesenjangan tersebut memunculkan pertanyaan yang belum terjawab, apakah kepatuhan sebuah organisasi terhadap regulasi pelindungan data pribadi selalu mencerminkan kematangan teknis keamanan informasinya. Penelitian terdahulu cenderung mengevaluasi Indeks KAMI dan kepatuhan hukum secara terpisah, sehingga hubungan antara keduanya pada satu entitas yang sama belum dipetakan secara sistematis. Padahal, kewajiban normatif dalam UU PDP pada praktiknya bertumpu pada kontrol teknis yang justru dinilai oleh Indeks KAMI. Penelitian ini menutup kesenjangan tersebut dengan memetakan keterkaitan antara persyaratan pasal-pasal UU PDP dan area penilaian Indeks KAMI 5.0, sehingga kepatuhan prosedural dapat diuji berdampingan dengan kematangan teknis. Inilah yang membedakan penelitian ini dari studi Indeks KAMI terdahulu yang bersifat murni evaluatif.

Berdasarkan hal tersebut, penelitian ini bertujuan mengevaluasi tingkat kematangan keamanan informasi dan kepatuhan hukum *platform* EdTech PT XYZ dalam pemrosesan data pribadi, dan memetakan keterkaitan antara persyaratan UU PDP dan area penilaian Indeks KAMI 5.0 untuk mengidentifikasi area yang perlu diperbaiki. Berdasarkan hasil evaluasi, rekomendasi perbaikan disusun mengacu pada ISO/IEC 27002:2022 yang memberikan pedoman kontrol keamanan informasi yang terstruktur dan komprehensif, mencakup enkripsi data, pengelolaan akses, dan manajemen insiden keamanan informasi. Penelitian ini memberikan dua kontribusi utama: secara akademis menyediakan pemetaan kesenjangan legal-teknis (*compliance-maturity gaps*) yang belum banyak dieksplorasi dalam literatur, dan secara praktis menawarkan rekomendasi yang dapat diadopsi oleh platform EdTech lain guna meningkatkan kematangan keamanan sekaligus memenuhi mandat UU PDP.

II. METODE

Evaluasi terhadap platform EdTech PT. XYZ dilakukan dengan menggunakan pendekatan studi kasus kualitatif. Dalam pelaksanaannya, penelitian ini terdiri atas beberapa tahapan, seperti ditunjukkan pada **Error! Reference source not found.**.



Gambar 1. Tahapan Penelitian

A. *Identifikasi Masalah*

Pada tahap ini dilakukan identifikasi terhadap permasalahan yang terjadi pada platform EdTech. Beberapa serangan ditemukan selama proses beta testing platform.

Kondisi tersebut disebabkan oleh adanya celah keamanan pada plugin WordPress yang digunakan oleh pengembang, sehingga menimbulkan kekhawatiran terhadap potensi risiko kebocoran data pribadi pengguna.

B. Pemilihan Responden

Pada tahap ini, metode *purposive sampling* digunakan untuk memperoleh pemahaman mendalam terhadap fenomena yang bersifat kompleks dan kontekstual sesuai dengan pendekatan penelitian kualitatif [21],[22]. Responden penelitian terdiri atas tiga pemangku kepentingan pada *Platform EdTech*, yaitu: *Chief Executive Officer* (CEO), *Chief Technology Officer* (CTO), dan *Vice President* (VP) *of Information Security & Application Management*.

C. Pengumpulan Data

Pengumpulan data dilakukan melalui metode kuesioner berbasis instrument Indeks KAMI 5.0 dengan fokus evaluasi pada empat area yang berkaitan langsung dengan pelindungan data pribadi, yaitu: Sistem Elektronik, Teknologi dan Keamanan Informasi, Pelindungan Data Pribadi, serta Pengelolaan Risiko Keamanan Informasi. Disamping itu, pertanyaan disusun berdasarkan pasal-pasal dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) yang mencakup substansi utama sebagai pengendalian data pribadi untuk menilai tingkat kepatuhan platform terhadap regulasi tersebut, meliputi:

- Jenis Data Pribadi (Pasal 4),
- Hak Subjek Data Pribadi (Pasal 5–13),
- Pemrosesan Data Pribadi (Pasal 16 dan 18), dan
- Kewajiban Pengendali Data Pribadi (Pasal 20–22, 24, 27–33, dan 35–47).

Dalam pengumpulan data ini, terdapat beberapa tahapan yang dilakukan sebagai berikut:

1. Pengelompokan Kategori Pada Instrumen Indeks KAMI

Setiap instrumen pertanyaan dikelompokkan berdasarkan kategori pengamanan (KP) dan tingkat kematangan untuk memberikan gambaran yang komprehensif mengenai penerapan keamanan informasi. Kategori pengamanan merefleksikan sejauh mana elemen-elemen pengamanan telah diimplementasikan, dimana masing-masing kategori mempresentasikan tahapan berbeda dalam proses pencapaian tingkat kematangan keamanan informasi sesuai dengan standar ISO/IEC 27001:2022. Adapun, terdapat tiga kategori pengamanan, yaitu:

- Kategori 1: Kerangka Kerja Dasar Keamanan Informasi
- Kategori 2: Penerapan Tingkat Efektivitas dan Konsistensi Penerapan
- Kategori 3: Kemampuan untuk Mengelola Risiko Keamanan Informasi.

Sementara itu, tingkat kematangan mencerminkan sejauh mana penerapan keamanan informasi telah dilaksanakan. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di suatu organisasi. Tingkat kematangan tersebut didefinisikan sebagai berikut [13]:

- Tingkat I: Kondisi Awal
- Tingkat II: Penerapan Kerangka Kerja Dasar
- Tingkat III: Terdefinisi dan Konsisten
- Tingkat IV: Terkelola dan Terukur
- Tingkat *V: Optimal*

2. Melakukan Penilaian Skor Terhadap Nilai Matriks

a. Matriks Kategori Pengamanan

Setiap pertanyaan dalam setiap area dikategorikan ke dalam tiga Kategori Pengamanan (KP), skor yang diperoleh akan semakin besar seiring dengan meningkatnya kategori pengamanan dan status penerapan yang lebih tinggi [13],[14]. Matriks yang digunakan untuk evaluasi ini dapat dilihat pada **Error! Reference source not found.**.

TABEL 1.
MATRIKS KATEGORI PENGAMANAN

Status Penerapan	Kategori Pengamanan		
	Kategori 1	Kategori 2	Kategori 3
Tidak dilakukan	0	0	0
Dalam perencanaan	1	2	3
Dalam Penerapan/Diterapkan Sebagian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9

b. Matriks Tingkat Kesiapan

Tingkat kesiapan didapati berdasarkan hasil dari perhitungan skor dari status pada area kategori sistem elektronik dan skor akhir dari setiap area yang telah dievaluasi [13],[14]. Matriks yang digunakan untuk evaluasi ini dapat dilihat pada **Error! Reference source not found.**.

TABEL 2.
MATRIKS TINGKAT KESIAPAN

Kategori Sistem Elektronik				Status Kesiapan
Rendah		Skor Akhir		
10	15	0	247	Tidak Layak
		248	443	Pemenuhan Kerangka Kerja Dasar
		444	760	Cukup Baik
		761	916	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	387	Tidak Layak
		388	646	Pemenuhan Kerangka Kerja Dasar
		647	828	Cukup Baik
		829	916	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	472	Tidak Layak
		473	760	Pemenuhan Kerangka Kerja Dasar
		761	864	Cukup Baik
		865	916	Baik

c. Matriks Level Tingkat Kematangan

Indeks KAMI mengembangkan sembilan level tingkat kematangan dengan menambahkan atribut ”+” pada setiap level, seperti I+, II+, hingga IV+, agar penilaian lebih granular . Atribut "+" ini digunakan untuk menunjukkan bahwa tingkat kematangan sudah berada di antara dua level, meskipun belum mencapai skor yang ideal. Apabila akumulasi skor hanya mencapai batas minimum suatu level, maka tingkat kematangan dikategorikan sebagai level "+" dari tingkat sebelumnya, yang merepresentasikan adanya peningkatan meskipun belum signifikan [13],[14].

D. Pemetaan Keterkaitan UU PDP dan Indeks KAMI

Pada tahap ini untuk memahami hubungan antara kepatuhan hukum dan kematangan teknis, dilakukan pemetaan (*crosswalk malpping*) antara pasal-pasal UU PDP yang dievaluasi dengan area penilaian Indeks KAMI 5.0. Adapun pemetaan dilakukan melalui tiga langkah berikut.

1. *Identifikasi substansi pasal*

Setiap pasal UU PDP yang dievaluasi (Pasal 4; 5–13; 16 dan 18; 20–22, 24, 27–33, dan 35–47) diuraikan menjadi kewajiban kendali (*control obligation*) yang bersifat konkret, misalnya kewajiban memperoleh persetujuan, kewajiban menyediakan mekanisme keberatan, atau kewajiban melaporkan insiden kebocoran data.

2. *Penautan terhadap kategori pengamanan Indeks KAMI*

Setiap kewajiban kendali tersebut ditautkan ke pertanyaan pada area Indeks KAMI yang secara substantif merepresentasikan implementasi teknis dari kewajiban tersebut. Sebagai contoh, kewajiban pelaporan insiden pelanggaran data (Pasal 46) ditautkan dengan pertanyaan pada area Pengelolaan Risiko Keamanan Informasi terkait prosedur penanganan insiden; kewajiban memperoleh persetujuan (Pasal 20–21) ditautkan dengan pertanyaan pada area Pelindungan Data Pribadi terkait mekanisme *consent.*

3. *Validasi pemetaan oleh pakar*

Hasil pemetaan awal diperiksa ulang oleh responden VP *of Information Security & Application Management* untuk memastikan kesesuaian antara substansi hukum dan substansi teknis, mengingat pemetaan bersifat konseptual dan berpotensi subjektif jika hanya dilakukan oleh peneliti.

E. Validasi Data

Tahap validasi data dilakukan untuk memastikan keakuratan dan konsistensi informasi yang diperoleh. Validasi dilakukan melalui verifikasi dokumen pendukung dan konfirmasi hasil wawancara dengan responden, khususnya jika status penerapan yang dilaporkan adalah "Dalam Penerapan/Diterapkan Sebagian" atau "Diterapkan Menyeluruh". Apabila tidak ditemukan bukti pendukung yang memadai untuk item pada kategori keamanan informasi, status tersebut diturunkan menjadi "Dalam Perencanaan" [14].

F. Analisis Data dan Rekomendasi

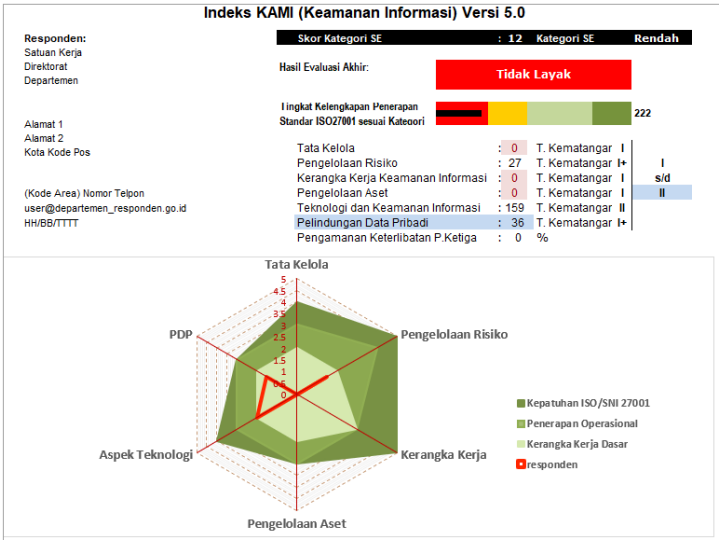
Proses analisis hasil evaluasi dilakukan dengan menggunakan matriks penilaian dari Indeks KAMI 5.0. Sementara itu, penilaian terhadap kepatuhan UU PDP dilakukan berdasarkan fitur dan mekanisme pengelolaan data pribadi yang tersedia pada platform. Kedua hasil evaluasi tersebut kemudian dianalisis secara berdampingan dengan mengacu pada pemetaan keterkaitan yang telah disusun pada bagian D, sehingga kesenjangan antara status kepatuhan dan status kematangan pada setiap area terkait dapat diidentifikasi secara sistematis. Berdasarkan hasil pemetaan tersebut, rekomendasi disusun dengan mengacu pada pedoman ISO/IEC 27002:2022 guna memperkuat pengelolaan keamanan informasi secara menyeluruh [23],[24].

III. HASIL DAN PEMBAHASAN

Hasil evaluasi terhadap aspek keamanan dan kepatuhan platform *EdTech* PT.XYZ, menunjukkan adanya perbedaan yang signifikan antara hasil penilaian kepatuhan hukum berdasarkan UU PDP dan tingkat kematangan teknis berdasarkan Indeks KAMI 5.0. Dari sisi kepatuhan hukum, platform menunjukkan tingkat penerapan yang tinggi, di mana 28 dari 36 pasal relevan dinilai "Diterapkan Sepenuhnya". Akan tetapi, penilaian dari sisi kematangan justru menempatkan platform pada level "Tidak Layak", dengan total skor akhir 222.

A. Hasil Evaluasi Indeks KAMI 5.0

Hasil evaluasi tingkat kematangan keamanan informasi terhadap *platform EdTech* menggunakan Indeks KAMI 5.0 disajikan dalam bentuk dashboard visual yang ditampilkan pada **Error! Reference source not found.**.



Gambar 2. Hasil Evaluasi Indeks KAMI

Berdasarkan hasil evaluasi pada Gambar 2 tersebut, *platform EdTech* PT.XYZ berada pada level ”Tidak Layak” dengan total skor akhir sebesar 222, dimana skor tertinggi diperoleh pada area Teknologi dan Keamanan Informasi, meskipun tingkat kematangannya masih berada pada level II. Adapun dua area lainnya yaitu Pengelolaan Risiko dan

Pelindungan Data Pribadi (PDP) menunjukkan skor kematangan yang lebih rendah yakni berada pada level I+.

Kategori Sistem Elektronik menunjukkan pola yang khas organisasi tahap awal (early-stage): dari 10 pertanyaan, hanya satu yang berstatus Tinggi, kepatuhan terhadap regulasi nasional. Sementara delapan lainnya berstatus Rendah karena aset sistem dan data yang dikelola masih tergolong sederhana. Pola ini bukan semata kegagalan keamanan, melainkan cerminan tahap pertumbuhan organisasi yang skala operasinya belum menuntut kompleksitas sistem elektronik yang tinggi.
Pada Pengelolaan Risiko, skor 27 dari batas minimum 40 untuk validasi Tahap Penerapan 3 mengindikasikan bahwa PT XYZ sudah memahami kerangka kerja risiko secara konseptual ambang batas risiko dan penanggung jawab aset sudah ditetapkan, namun belum mengoperasionalkannya menjadi siklus mitigasi yang terdokumentasi dan dikaji berkala. Dengan kata lain, kesenjangan berada pada tahap implementasi, bukan pada tahap pemahaman.

Teknologi dan Keamanan Informasi mencatat skor tertinggi relatif (159, Tingkat Kematangan II) karena PT XYZ telah menerapkan kontrol teknis dasar (standar OWASP 10, antivirus, pembaruan aplikasi berkala). Namun, validasi Tahap Penerapan 3 tetap gagal karena ketiadaan audit independen berkala dan mekanisme Data Leakage Prevention — kedua hal ini bersifat governance (pengawasan pihak ketiga dan kebijakan proaktif), bukan sekadar kontrol teknis, sehingga menunjukkan bahwa kapasitas teknis PT XYZ melampaui kematangan tata kelolanya.

Pelindungan Data Pribadi mencatat skor terendah kedua (36, Tingkat Kematangan I+), dengan pola yang konsisten: dua item krusial berorientasi hak pengguna (persetujuan, akses data) sudah diterapkan penuh, tetapi penunjukan fungsi penanggung jawab pelindungan data pribadi dan prosedur pengungkapan data kepada aparat penegak hukum sama sekali belum ada. Ini adalah temuan penting karena area inilah yang secara substantif paling dekat dengan kewajiban UU PDP, sehingga skor rendahnya berimplikasi langsung terhadap risiko kepatuhan hukum, bukan hanya risiko teknis.

B. Hasil Evaluasi UU PDP

Evaluasi kepatuhan platform PT XYZ terhadap 36 pasal relevan dalam Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menunjukkan bahwa 29 pasal telah Diterapkan Sepenuhnya, 3 pasal Diterapkan Sebagian, dan 4 pasal Tidak Diterapkan (Tabel 10). Keempat pasal yang sama sekali belum diimplementasikan mencakup Pasal 10 terkait prosedur hak keberatan pengguna, Pasal 12 mengenai ganti rugi pelanggaran data, Pasal 40 tentang batas waktu penghentian pemrosesan (penarikan persetujuan) maksimal 3×24 jam yang saat ini masih memakan waktu hingga tiga bulan di PT XYZ, serta Pasal 46 mengenai kewajiban pelaporan kegagalan pelindungan data maksimal 3×24 jam. Ketiadaan prosedur formal pada situasi-situasi ini berpotensi memunculkan masalah transparansi dan akuntabilitas. Oleh karena itu, PT XYZ disarankan untuk segera membentuk tim legal khusus, meninjau ulang kategorisasi data pribadi yang disimpan, serta merumuskan Standard Operating Procedure (SOP) penanganan insiden dan penarikan data sesuai tenggat waktu regulasi.

Selain itu, evaluasi menemukan tiga pasal yang baru diterapkan secara parsial. Pada Pasal 16, PT XYZ belum mendokumentasikan kebijakan retensi penyimpanan maupun prosedur pemberitahuan kegagalan pemrosesan. Pada Pasal 32 yang mengatur hak subjek atas riwayat pemrosesan, platform baru menyediakan fitur unduh data pembayaran dan kuis, namun belum mengakomodasi pengunduhan data profil dan riwayat aktivitas (*login*). Selanjutnya, pemenuhan Pasal 47 terkait pertanggungjawaban data juga dinilai belum maksimal; meskipun teknologi yang digunakan sudah memadai, entitas belum memiliki kerangka kerja tata kelola perlindungan data dan unit penanggung jawab khusus. Peneliti merekomendasikan pelaksanaan audit internal untuk menyusun kebijakan retensi data, pengembangan fitur riwayat *login* bagi pengguna, serta pembentukan tata kelola dokumentasi formal.

Secara keseluruhan, keberhasilan penerapan 29 pasal (termasuk Pasal 5 terkait informasi identitas di Kebijakan Privasi) menunjukkan bahwa kepatuhan platform cukup kuat pada aspek operasional rutin yang melekat pada alur kerja produk. Sebaliknya, 7 pasal yang belum terpenuhi mengungkap dua kelemahan mendasar organisasi, yakni kurangnya pemahaman integratif terhadap prinsip tata kelola pelindungan (Pasal 16, 32, dan 47), serta ketidaksiapan menghadapi situasi insidental di luar operasional harian (Pasal 10, 12, 40, dan 46). Pola ini mengindikasikan bahwa kepatuhan PT XYZ terbentuk secara reaktif guna memenuhi fungsionalitas produk semata, bukan dirancang secara proaktif dari kerangka manajemen risiko yang terstruktur. Temuan ini menjadi faktor penyebab yang sejalan dan konsisten dengan rendahnya skor Pengelolaan Risiko pada hasil evaluasi Indeks KAMI.

C. Analisis Pemetaan UU PDP terhadap Indeks KAMI

Pemetaan dilakukan sebagai respons terhadap ketidakseimbangan hasil antara evaluasi kepatuhan terhadap UU PDP dan skor Indeks KAMI. Meskipun PT XYZ dinilai telah menerapkan sebagian besar pasal dalam UU PDP, hasil audit Indeks KAMI justru menunjukkan skor rendah, khususnya pada area Pengelolaan Risiko dan Pelindungan Data Pribadi yang berada pada level I+.

Dari total 36 pasal yang relevan dengan peran PT XYZ sebagai Pengendali Data Pribadi, hasil pemetaan menunjukkan bahwa tidak semua pasal memiliki padanan langsung dengan instrumen dalam Indeks KAMI. Ringkasan pemetaan disajikan pada Tabel 3 berikut.

TABEL 3.
PEMETAAN UU PDP TERHADAP INDEKS KAMI

Kelompok Pasal (Substansi)	Σ Pasal	Area KAMI Dominan	Ada Padanan	Tanpa Padanan
Jenis Data Pribadi (Pasal 4)	1	I. Sistem Elektronik	1	0

Hak Subjek Data Pribadi (Pasal 5–13)	9	VII. Pelindungan Data Pribadi	4	5 (Pasal. 6, 9, 10, 11, 13)
Pemrosesan Data Pribadi (Pasal 16, 18)	2	I, VI, VII	2	0
Kewajiban Pengendali Data (Pasal 20–47)	24	III, VI, VII	23	1 (Pasal. 41)
Total	36	—	30	6

Hasil pemetaan menunjukkan pola yang tidak merata: dari 36 pasal yang dievaluasi, 30 pasal (83%) memiliki padanan instrumen pada Indeks KAMI, namun kesenjangan terkonsentrasi tajam pada kelompok Hak Subjek Data Pribadi (Pasal 5–13), di mana 5 dari 9 pasal (56%) tidak memiliki padanan sama sekali. Sebaliknya, kelompok Kewajiban Pengendali Data (Pasal 20–47) yang bersifat lebih operasional dan teknis, hampir seluruhnya terpetakan (23 dari 24 pasal). Pola ini konsisten dengan perbedaan orientasi kedua kerangka: Indeks KAMI dibangun di atas standar ISO/IEC 27001 yang menilai kesiapan sistem dan tata kelola, sehingga kuat pada kewajiban prosedural pengendali data, tetapi belum secara eksplisit menginstrumentasi hak individual subjek data yang bersifat reaktif terhadap permintaan pengguna. Seperti menarik persetujuan, mengajukan keberatan, atau meminta portabilitas data. Kesenjangan struktural inilah, bukan sekadar kelemahan implementasi, yang menjelaskan mengapa kepatuhan prosedural terhadap UU PDP dapat tampak tinggi sementara kematangan Indeks KAMI tetap rendah — celah tersebut sebagian berasal dari cakupan instrumen itu sendiri, bukan semata dari kegagalan organisasi.

IV. REKOMENDASI

Berdasarkan hasil evaluasi Indeks KAMI dan kepatuhan UU PDP, rekomendasi perbaikkan disusun mengacu pada ISO/IEC 27002:2022, sebagaimana dirangkum pada Tabel 4. Dengan mempertimbangkan keterbatasan sumber daya PT XYZ sebagai organisasi rintisan, satu rekomendasi ditetapkan sebagai prioritas utama: penunjukan resmi Penanggung Jawab Keamanan Data dan Privasi (DPO/PIC), dengan alasan sebagai berikut:

a) Memberikan arah dan akuntabilitas yang jelas atas program pelindungan data, yang selama ini belum terstruktur.
b) Ketiadaan tata kelola formal adalah akar penyebab bersama dari rendahnya skor Pengelolaan Risiko Indeks KAMI dan ketidakpatuhan pada pasal-pasal insidental UU PDP, sebagaimana diuraikan pada analisis pemetaan.
c) Berbiaya relatif rendah karena dapat dimulai melalui peran ganda karyawan internal yang kompeten, sehingga realistis untuk organisasi tahap awal.
d) Menjadi prasyarat keberhasilan rekomendasi teknis lain — tanpa peran ini, perbaikan berisiko tidak terimplementasi secara konsisten.

Rekomendasi ini sekaligus berfungsi sebagai model implementasi minimum yang dapat diadopsi organisasi EdTech lain dengan karakteristik serupa (skala kecil, sumber daya terbatas, tahap pertumbuhan awal): mulai dari penunjukan penanggung jawab, dilanjutkan dengan dokumentasi kebijakan pelindungan data, dan diakhiri dengan penguatan kontrol teknis sesuai prioritas risiko masing-masing organisasi.

TABEL 4.
REKOMENDASI PERBAIKAN

Sumber Temuan	Isu Utama	Kontrol ISO/IEC 27002:2022	Rekomendasi Inti
UU PDP (Pasal 10, 40)	Belum ada mekanisme penarikan persetujuan/keberatan yang terprosedur	5.31 Legal, statutory, regulatory and contractual requirements	PIA, fitur opt-out, SOP penanganan penarikan persetujuan (SLA 3×24 jam)
UU PDP (Pasal 12, 46)	Belum ada dokumentasi kewajiban ganti rugi & pelaporan insiden		Dokumentasi kewajiban hukum, sistem manajemen insiden (mis. JIRA)
KAMI — Pengelolaan Risiko (I+)	Kerangka kerja risiko belum terdokumentasi & belum ada penanggung jawab formal	5.1 Policies for Information Security	Program pengelolaan risiko terstruktur, penunjukan CISO/tim keamanan, inventarisasi aset, metrik KPI (MTTR)
KAMI — Teknologi & Keamanan Informasi (II)	Infrastruktur belum redundan untuk kontinuitas layanan	5.30 ICT Readiness for Business Continuity	Server clustering, replikasi data real-time, Disaster Recovery Plan
KAMI — Pelindungan Data Pribadi (I+)	Dokumentasi kebijakan & fungsi penanggung jawab pelindungan data belum ada	5.9 Inventory of Information	Personal Data Flow (PDF) mapping, penunjukan fungsi/pejabat pelindung data pribadi

IV. KESIMPULAN

Isu keamanan data pribadi menjadi tantangan krusial di sektor pendidikan digital Indonesia. Urgensi ini nyata dialami PT XYZ, yang sempat mengalami percobaan serangan siber (*backlink* dan *backshell*) selama tahap uji coba beta platform.

Penelitian ini mengevaluasi kematangan keamanan informasi PT XYZ menggunakan Indeks KAMI 5.0 dan kepatuhannya terhadap UU PDP, sekaligus memetakan keterkaitan antara kedua kerangka tersebut. Hasil evaluasi Indeks KAMI menunjukkan skor akhir 222 dengan status "Tidak Layak", terutama lemah pada area Pengelolaan Risiko dan Pelindungan Data Pribadi (Level I+). Sementara itu, dari 36 pasal UU PDP yang dievaluasi, 29 pasal diterapkan sepenuhnya, 3 pasal diterapkan sebagian, dan 4 pasal tidak diterapkan sama sekali. Kesenjangan antara kedua hasil ini bukan paradoks, melainkan cerminan perbedaan orientasi mendasar. UU PDP menekankan perlindungan hak subjek data secara normatif, sedangkan Indeks KAMI menilai kesiapan teknis dan tata kelola. Hasil pemetaan pada penelitian ini memperjelas bahwa sebagian kesenjangan tersebut juga bersifat struktural, 5 dari 9 pasal terkait Hak Subjek Data Pribadi tidak memiliki padanan instrumen pada Indeks KAMI. Sehingga kepatuhan administratif yang tinggi tidak serta-merta mencerminkan kematangan keamanan yang menyeluruh.

Sebagai wujud kontribusi penelitian, hasil pemetaan sistematis ini secara teoretis mengisi celah literatur terkait integrasi instrumen teknis KAMI dan regulasi hukum yang belum banyak dieksplorasi. Secara praktis, penelitian ini menawarkan model implementasi dasar bagi organisasi EdTech, seperti penunjukan Penanggung Jawab Keamanan Data (*Data Protection Officer*) dan pengadopsian kontrol

keamanan berbasis ISO/IEC 27002:2022. Guna menyelaraskan peningkatan kematangan teknis dengan kepatuhan UU PDP secara berkesinambungan.

Penelitian ini memiliki keterbatasan sebagai studi kasus tunggal pada satu platform EdTech berskala rintisan, sehingga temuan kuantitatif (skor dan persentase kepatuhan) tidak dapat digeneralisasi secara langsung ke organisasi EdTech berskala lebih besar atau dengan model bisnis berbeda. Namun, pola kesenjangan struktural antara UU PDP dan Indeks KAMI yang teridentifikasi bersifat konseptual dan berpotensi relevan bagi organisasi EdTech lain dengan karakteristik serupa, khususnya yang berada pada tahap pertumbuhan awal dengan tata kelola privasi yang belum matang.

DAFTAR PUSTAKA

[1] D. Kim, K. Borowiec, and S. Wortham, “A New Era in EdTech: Emerging Challenges and Opportunities,” *ECNU Review of Education*, vol. 7, no. 2, 2023, doi: 10.1177/20965311231200510.

[2] Badan Siber dan Sandi Negara, "Laporan Landscape Keamanan Siber Indonesia 2023," Jakarta, Badan Siber dan Sandi Negara, 2023. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf. [Accessed: Oct. 5, 2024].

[3] A. Zeyab and G. M. Alayyar, “Perspective Chapter: Education Technology (EdTech) and the Online Course Revolution,” *IntechOpen*, 2023, doi: 10.5772/intechopen.109227.

[4] A. S. Al-Sherideh, K. Maabreh, M. Maabreh, M. R. A. Mousa, and M. Asassfeh, "Assessing the impact and effectiveness of cybersecurity measures in e-learning on students and educators: A case study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 5, p. 159, 2023.

[5] Q. Liu and M. Khalil, “Understanding privacy and data protection issues in learning analytics using a systematic review,” *Br. J. Educ. Technol.*, vol. 54, no. 6, pp. 1–33, Sep. 2023, doi: 10.1111/bjet.13388.

[6] A. A. Rahman, A. Marwan, and A. T. Haryono, "The readiness for privacy compliance in Indonesia before October 2024," *Int. J. Soc. Sci. Human. Res.*, vol. 7, no. 8, pp. 6154-6155, 2024, doi: 10.47191/ijsshr/v7-i08-41.

[7] E. P. Maheswari and S. A. Wiraguna, “Urgensi Persetujuan Pemilik Data dalam Pengelolaan Data Pribadi oleh Platform Digital”, *JIKSP*, vol. 2, no. 4, pp. 908–914, 2025. [Online]. Available: http://jurnal.ittc.web.id/index.php/jiksp/article/view/2498.

[8] H. H. Samin, “Perlindungan hukum terhadap kebocoran data pribadi oleh pengendali data melalui pendekatan hukum progresif,” *J. Ilm. Res. Student*, vol. 1, no. 3, 2023, doi: 10.61722/jssr.v1i3.386.

[9] Undang-Undang Republik Indonesia, “Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi”, Jakarta: Presiden Republik Indonesia, 2022.

[10] Tim Pengukuran Tingkat Kematangan Keamanan Siber dan Sandi, "Pedoman Pengisian Instrumen Indeks KAMI v5.0 Pemerintah Daerah," Direktorat Keamanan Siber dan Sandi Pemerintah Daerah, Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia, Badan Siber dan Sandi Negara (BSSN), Revisi 2.0, Apr. 2025.

[11] K. Wasilah, M. S. H. Kurniawan, and Firmansyah, "Evaluasi Tingkat Keamanan Informasi Pada Dinas Kominfo Lampung Selatan Menggunakan Indeks Kami 4.3," *Jurnal Ilmu Komputer Agri-informatika*, vol. 11, no. 1, pp. 13–18, 2022. [Online]. Available: https://journal.ipb.ac.id/index.php/jika.

[12] H. I. Azmi, M. T. Akbar, B. T. Kumala Dewi, and B. Sugiantoro, "Evaluasi Tingkat Kesiapan Keamanan Informasi Pada SMK XYZ Menggunakan Indeks KAMI Versi 4.2," *CyberSecurity dan Forensik Digital*, vol. 7, no. 1, pp. 42–49, 2024, doi: 10.14421/csecurity.2024.7.1.4422.

[13] M. S. Jenny, R. N. Shofa, and A. Rahmatulloh, "Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Keamanan Informasi (Indeks KAMI) Versi 4.2 Pada Sistem Informasi Akademik (SIMAK) Universitas Siliwangi," *Jurnal Sistem Informasi dan Teknologi*, vol. 7, no. 1, pp. 1-10, 2024, doi: 10.24176/sitech.v7i1.12390.

[14] D. I. Khamil, G. M. A. Sasmita, and A. A. H. Susila, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 3, pp. 1948–1960, 2022, doi: 10.35957/jatisi.v9i3.2310.

[15] S. Yuliani, N. T. Ramadhini, A. I. Gustisyaf, and A. Wahyudin, "Asesmen Keamanan Informasi Menggunakan Indeks KAMI," *NARATIF (Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika)*, vol. 2, no. 1, pp. 1-10, 2020, doi: 10.53580/naratif.v2i1.76.

[16] M. Rizkillah, "Evaluasi Keamanan Informasi Perguruan Tinggi Menggunakan Indeks Keamanan Informasi (KAMI) Versi 5.0," *Jurnal Cakrawala Ilmiah*, vol. 3, no. 10, pp. 1-10, 2024, doi: 10.54099/jci.v3i10.7988.

[17] L. D. A. Jelita, M. N. A. Azam, and A. Nugroho, "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022," *Jurnal Saintekom: Sains, Teknologi, Komputer dan Manajemen*, vol. 14, no. 1, pp. 84–94, 2024, doi: 10.33020/saintekom.v14i1.623.

[18] A. L. Maryanto, M. N. A. Azam, and A. Nugroho, "Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks KAMI," *Jurnal Simantec*, vol. 11, no. 1, pp. 1-10, 2022, doi: 10.21107/simantec.v11i1.14099.

[19] S. F. Rahayu, D. Prawira, and I. Rusi, "Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks KAMI (Studi Kasus: Dinas Komunikasi dan Informatika Kota Pontianak)," *Jurnal Komputer dan Aplikasi*, vol. vol. 9, no. 3, pp. 468–477, 2021, doi: 10.26418/coding.v9i03.51126.

[20] D. Saputra, R. Y. Rahman, M. S. Hasibuan, and G. J. H. Aziz, "Penilaian Tingkat Kesiapan Keamanan Informasi Pada Dinas Kominfo Kabupaten XYZ dengan Indeks KAMI Versi 4.2," *Jurnal Ilmu Komputer, Sistem Informasi, Teknik Informatika*, vol. 2, no. 2, pp. 1–10, Sep. 2023. [Online]. Available: https://jurnal.akommedia.net/index.php/JILKOMSITI/article/view/31.

[21] O. Tajik, J. Golzar, and S. Noor, “Purposive Sampling,” *Int. J. Educ. Lang. Stud.*, vol. 2, no. 2, pp. 85–92, 2024, doi: 10.59569/ijels.v2i2.411.

[22] J. Ani, B. Lumanauw, and J. L. A. Tampenawas, "Pengaruh citra merek, promosi dan kualitas layanan terhadap keputusan pembelian konsumen pada e-commerce Tokopedia di Kota Manado," *J. EMBA*, vol. 10, no. 1, pp. 667–676, 2022, doi: 10.35794/emba.v10i1.38279.

[23] B. S. Wibowo and R. F. Aji, "Rekomendasi implementasi 11 kontrol keamanan informasi baru ISO/IEC 27001:2022 di perusahaan HealthTech XYZ," *The Indonesian Journal of Computer Science*, vol. 13, no. 4, pp. 315–325, 2024, doi: 10.33022/ijcs.v13i4.4166.

[24] K. S. A. Fajri and R. Harwahyu, “Information Security Management System Assessment Model by Integrating ISO 27002 and 27004”, *MALCOM*, vol. 4, no. 2, pp. 498-506, Feb. 2024.