EFEKTIVITAS SISTEM PENGENDALIAN INTERNAL (COSO) DALAM MENJAMIN KEPATUHAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI (UU PDP) DI SEKTOR PERBANKAN INDONESIA

Media Muharram
Universitas Padjajaran
pos-el: media24001@mail.unpad.ac.id

ABSTRAK

Perkembangan digital di sektor perbankan membawa tantangan baru dalam menjaga keamanan dan kerahasiaan data nasabah. Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menuntut bank untuk memiliki tata kelola data yang transparan, sistematis, dan sesuai prinsip akuntabilitas. Dalam konteks ini, Sistem Pengendalian Internal (SPI) yang berlandaskan pada kerangka COSO (Committee of Sponsoring Organizations of the Treadway Commission) menjadi instrumen penting untuk memastikan kepatuhan terhadap regulasi serta meminimalkan risiko kebocoran data pribadi. Penelitian ini bertujuan untuk menganalisis efektivitas penerapan sistem pengendalian internal berbasis COSO dalam menjamin kepatuhan terhadap UU PDP di sektor perbankan Indonesia. Melalui pendekatan studi literatur, penelitian ini menelaah hasil-hasil empiris dan konseptual terkait hubungan antara komponen COSO yakni lingkungan pengendalian, penilaian risiko, aktivitas pengendalian, informasi dan komunikasi, serta pemantauan dengan mekanisme perlindungan data pribadi di lembaga keuangan. Hasil kajian menunjukkan bahwa efektivitas SPI COSO sangat bergantung pada dukungan manajemen puncak, budaya kepatuhan organisasi, serta kesadaran sumber daya manusia terhadap pentingnya keamanan data. Komponen Control Environment dan Monitoring berperan dominan dalam membangun sistem pelaporan dan audit yang mampu mendeteksi pelanggaran sejak dini, sedangkan Information and Communication menjadi kunci dalam memastikan transparansi pengelolaan data lintas unit kerja. Temuan ini menegaskan bahwa keberhasilan implementasi UU PDP tidak hanya ditentukan oleh regulasi yang kuat, tetapi juga oleh kualitas penerapan pengendalian internal dan kesiapan SDM dalam mengelola risiko informasi. Dengan demikian, kerangka COSO dapat berfungsi sebagai pendekatan integratif yang memperkuat tata kelola, akuntabilitas, serta kepercayaan publik terhadap institusi perbankan di era digital.

Kata kunci : Sistem Pengendalian Internal, COSO, UU PDP, Kepatuhan, Keamanan Data, Sektor Perbankan.

ABSTRACT

The rapid digitalization of Indonesia's banking sector has introduced new challenges in safeguarding customer data and ensuring compliance with evolving privacy regulations. The enforcement of Law No. 27 of 2022 on Personal Data Protection (PDP Law) requires banks to strengthen governance systems and implement strict security measures to protect customer information. In this context, the Internal Control System (ICS) based on the COSO framework (Committee of Sponsoring Organizations of the Treadway Commission) plays a crucial role in ensuring regulatory compliance and minimizing the risk of data breaches. This study aims to analyze the effectiveness of COSO-based internal controls in ensuring compliance with the PDP Law within Indonesia's banking sector. Using a literature review approach, this research examines empirical and theoretical findings related to the five COSO components Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring and their alignment with data protection governance. The results indicate that the effectiveness of COSO implementation depends greatly on top management commitment, organizational compliance culture, and employee awareness regarding data security. The Control Environment and Monitoring components are critical for establishing early detection mechanisms, while Information and Communication ensures transparency and accountability in managing customer data across departments. This study concludes that compliance with the

PDP Law cannot be achieved through regulation alone; it requires the integration of robust internal controls and competent human resources capable of managing information risks effectively. The COSO framework thus provides an integrative approach to strengthening governance, accountability, and public trust in the banking sector's data management practices.

Keywords: Internal Control System, COSO, PDP Law, Compliance, Data Security, Banking Sector

1. PENDAHULUAN

Perkembangan teknologi digital telah mengubah lanskap industri perbankan secara signifikan. Layanan keuangan berbasis teknologi seperti mobile banking, dompet digital, dan sistem kredit online yang memberikan efisiensi yang tinggi dalam pengelolaan data dan pelayanan kepada nasabah. Sebagai contoh, penelitian di Pakistan menunjukkan bahwa mekanisme enkripsi dan keamanan data merupakan faktor utama dalam melindungi nasabah digital banking (Ahmed et al., 2024). Namun, di sisi lain, peningkatan volume dan kompleksitas data digital juga memperbesar risiko kebocoran informasi pribadi, yang dapat menimbulkan kerugian reputasi maupun legal bagi lembaga keuangan.

Di Indonesia, isu perlindungan data pribadi menjadi salah satu prioritas utama sektor perbankan, terutama sejak diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini menuntut lembaga keuangan untuk menerapkan sistem tata kelola data yang transparan, aman, dan bertanggung jawab termasuk memastikan bahwa seluruh proses pengumpulan, penyimpanan, dan pemrosesan data dilakukan berdasarkan prinsip consent, purpose limitation, dan accountability. Studi normatif menyebutkan bahwa meskipun kerangka regulasi telah hadir, tantangan seperti rendahnya kesadaran publik dan belum optimalnya mekanisme pengawasan tetap menjadi hambatan besar (Budiman, 2023).

Untuk menjamin kepatuhan terhadap UU PDP, setiap bank memerlukan Sistem Pengendalian Internal (SPI) yang kuat dan terintegrasi. Kerangka Committee of Sponsoring Organizations of the Treadway Commission (COSO) banyak diadopsi secara global sebagai acuan dalam merancang SPI yang efektif, dengan lima komponen utama: lingkungan pengendalian (control environment), penilaian risiko (risk assessment), kegiatan pengendalian (control activities), informasi dan komunikasi (information & communication), serta aktivitas monitoring (monitoring activities) (COSO, 2013). Meskipun literatur tentang COSO dan pengendalian internal telah banyak membahas risiko keuangan dan kecurangan, penerapannya dalam konteks perlindungan data pribadi terutama di perbankan masih relatif terbatas. Sebuah studi internasional mencatat bahwa kepatuhan kerangka internal control seperti COSO berpengaruh signifikan terhadap efektivitas pengendalian TI dan keamanan informasi. Namun, penelitian empiris di Indonesia menunjukkan bahwa efektivitas penerapan COSO dalam konteks perlindungan data masih bervariasi antar bank. Misalnya, sebagaian besar insiden pelanggaran data bukan semata disebabkan oleh kelemahan sistem teknologi, melainkan oleh rendahnya kesadaran dan kepatuhan pegawai terhadap kebijakan keamanan informasi. Dengan demikian, efektivitas SPI berbasis COSO tidak hanya bergantung pada desain sistem teknis, tetapi juga pada

perilaku dan budaya organisasi yang mendukung kepatuhan.

Dalam konteks perbankan Indonesia, penerapan COSO sebagai alat untuk memastikan kepatuhan UU PDP menghadapi sejumlah tantangan seperti keterbatasan kompetensi SDM dalam bidang keamanan data, kurangnya integrasi antar-unit kerja, serta belum optimalnya mekanisme monitoring dan pelaporan insiden. Oleh karena itu, penelitian ini menjadi relevan untuk mengevaluasi sejauh mana efektivitas Sistem Pengendalian Internal (COSO) dapat menjamin kepatuhan terhadap UU PDP di sektor perbankan Indonesia.

Penelitian ini juga diharapkan mampu memberikan pemahaman komprehensif mengenai hubungan antara pengendalian internal, kesadaran sumber daya manusia, dan keberhasilan penerapan regulasi perlindungan data pribadi. Dengan demikian, hasil kajian ini dapat menjadi dasar bagi manajemen perbankan dan regulator seperti Otoritas Jasa Keuangan (OJK) untuk memperkuat kebijakan tata kelola keamanan data di era digital yang semakin kompleks.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif-asosiatif dengan metode studi literatur untuk memetakan konsep dan temuan empiris terkait efektivitas sistem pengendalian internal berbasis COSO dalam mendukung penerapan perlindungan data pribadi sesuai UU PDP di sektor perbankan. Pendekatan deskriptif digunakan untuk menggambarkan konsep-konsep kunci seperti pengendalian internal, tata kelola data, dan literasi privasi SDM, sedangkan pendekatan asosiatif dipakai untuk mengidentifikasi hubungan konseptual antara efektivitas COSO, kesadaran tenaga pemasar, dan tingkat kepatuhan terhadap UU PDP. Analisis dilakukan secara konseptual untuk melihat sintesis teori COSO, regulasi perlindungan data, dan Information Privacy Management (IPM) Theory.

Pemilihan literatur dilakukan secara sistematis melalui database Scopus, ScienceDirect, Google Scholar, Taylor & Francis, SpringerLink, serta SINTA, dengan periode publikasi 2013–2025 agar tetap relevan dengan perkembangan modern keamanan data dan implementasi UU PDP. Dari hasil pencarian, penelitian ini menelaah 10 sumber ilmiah utama yang terdiri atas 7 jurnal internasional dan 3 literatur nasional berupa buku akademik, regulasi OJK, dan dokumen COSO 2013 Framework. Literatur dipilih menggunakan kata kunci seperti “COSO internal control,” “personal data protection compliance,” “banking data governance,” “IPM theory,” dan “data privacy awareness.” Hanya referensi yang memenuhi kriteria reputasi ilmiah, kesesuaian topik, serta relevansi konteks perbankan Indonesia yang digunakan sebagai dasar analisis.

Untuk menjamin validitas dan kredibilitas hasil penelitian, dilakukan tiga langkah verifikasi literatur, yaitu triangulasi sumber, evaluasi kredibilitas, dan peer review internal. Triangulasi dilakukan dengan membandingkan hasil temuan dari jurnal internasional, laporan regulator, dan pedoman COSO untuk memastikan konsistensi konsep. Evaluasi kredibilitas memastikan bahwa sumber yang digunakan berasal dari jurnal bereputasi atau regulasi yang sah. Peer review internal dilakukan melalui penelaahan ulang oleh rekan sejawat dan dosen pembimbing untuk menilai kesesuaian logika argumentasi, ketajaman

analisis, serta hubungan variabel yang disusun. Dengan pendekatan tersebut, penelitian ini diharapkan mampu menyediakan landasan konseptual yang kuat dalam menganalisis efektivitas sistem pengendalian internal dan kesadaran SDM terhadap keamanan pengelolaan data pribadi di Bank DKI.

3. HASIL DAN PEMBAHASAN

Penelitian ini menelaah 10 sumber ilmiah utama, terdiri dari 7 jurnal internasional dan 3 sumber buku/regulasi nasional. Berdasarkan hasil telaah, ditemukan bahwa penerapan Sistem Pengendalian Internal (COSO) secara signifikan mendukung kepatuhan organisasi terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP), terutama disertai dengan kesiapan dan kesadaran SDM yang tinggi.

Tabel 1. Ringkasan Hasil Studi Literatur Terkait COSO, SDM, dan Kepatuhan UU PDP

Peneliti (Tahun)	Fokus Penelitian	Temuan Utama	Relevansi dengan Penelitian Ini
(Onesti & Palumbo, 2023)	*Tone at the Top for Sustainable Corporate Governance to Prevent Fraud*	"Tone at the top" pimpinan sangat memengaruhi budaya etika & mekanisme pengendalian internal dalam mencegah fraud.	Menguatkan pentingnya komponen *Control Environment* dalam kerangka Committee of Sponsoring Organizations of the Treadway Commission (COSO) dan kaitannya dengan kepatuhan data pribadi.
(Kim et al., 2023)	*The Double-Edged Sword of Big Data and IT for the Disadvantaged: A Cautionary Tale from Open Banking*	Big data dan teknologi bank membuka peluang besar namun juga risiko privasi yang tersembunyi.	Konteks relevan untuk variabel teknologi & sistem dalam bank dan kepatuhan data pribadi.
(Kassem, 2022)	Elucidating Corporate Governance's Impact and Role in Fraud	Tata kelola korporasi efektif mengurangi risiko fraud.	Relevan untuk komponen *Control Environment* dan *Monitoring Activities* dalam COSO.
(Annastasyia Mukrimah Yusuf, Ma'ruf Hafidz, 2024)	Perlindungan hukum kerahasiaan data pribadi nasabah perbankan di Indonesia pasca UU No. 27 Tahun 2022	Menelaah tanggung jawab hukum dan tata kelola perbankan dalam menjaga kerahasiaan data pribadi nasabah setelah diberlakukannya UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)	Kewajiban menjaga kerahasiaan data nasabah kini menjadi tanggung jawab hukum substantif bagi lembaga perbankan

(Esther, 2022)	*Common Causes of Data Breaches in Banking and How to Mitigate Them*	Studi literatur: human error, teknologi usang, dan kelemahan kebijakan merupakan penyebab utama kebocoran data di perbankan.	Sangat relevan dengan variabel risk assessment dan control activities dalam kerangka COSO serta kepatuhan terhadap UU PDP.
(COSO, 2013)	*Internal Control – Integrated Framework*	Lima komponen utama pengendalian internal menjadi fondasi tata kelola risiko organisasi.	Kerangka dasar penelitian.
(Dewan Perwakilan Rakyat Republik Indonesia, 2022)	*Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*	Regulasi utama di Indonesia dengan prinsip consent, purpose limitation, accountability.	Regulasi utama dalam konteks kepatuhan perlindungan data pribadi (PDP).
(OJK, 2023)	*Laporan Kepatuhan Perbankan 2023*	Implementasi PDP di bank masih parsial, lebih terfokus TI, belum terintegrasi manajemen risiko.	Memberikan konteks empiris untuk bank di Indonesia, terutama relevan dengan penelitian di perbankan.
(Waliullah et al., 2025)	Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking	Ancaman siber signifikan terhadap adopsi digital banking dan kepatuhan regulasi.	Memberikan konteks terkini untuk perbankan digital dan kepatuhan data.
(Amoresano & Yankson, 2023)	Human Error – A Critical Contributing Factor to the Rise in Data Breaches	Human error menjadi salah satu penyebab utama pelanggaran data; pelatihan & kesadaran penting.	Menegaskan variabel kesadaran SDM/pegawai sebagai moderator penting dalam penelitian Anda terkait kepatuhan UU PDP.

Berdasarkan hasil kajian dari sepuluh sumber jurnal dan referensi terkait, efektivitas sistem pengendalian internal berbasis kerangka COSO menunjukkan hubungan erat dengan kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) di sektor perbankan. Onesti dan Palumbo (2023) menekankan bahwa kepemimpinan yang berintegritas (*tone at the top*) merupakan dasar bagi terciptanya lingkungan pengendalian (*control environment*) yang sehat, sejalan dengan temuan Kassem (2022) bahwa tata kelola perusahaan yang baik dapat menekan risiko kecurangan dan meningkatkan transparansi organisasi. Selaras dengan itu, Kim et al. (2023) mengingatkan bahwa perkembangan teknologi dan pemanfaatan *big data* dalam perbankan membawa manfaat efisiensi sekaligus meningkatkan risiko privasi, sehingga penerapan komponen COSO seperti *risk assessment* dan *monitoring activities*

menjadi semakin krusial. Di sisi lain, Amoresano dan Yankson (2023) serta Esther (2022) menyoroti bahwa faktor manusia masih menjadi penyebab dominan terjadinya pelanggaran data pribadi, sehingga kesadaran dan pelatihan sumber daya manusia perlu diperkuat sebagai bagian dari upaya kepatuhan terhadap UU PDP.

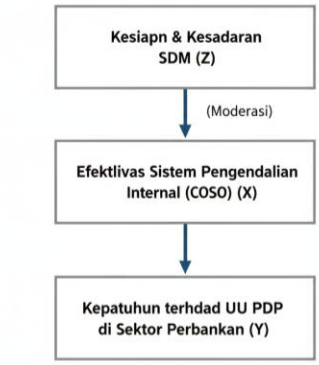
Sementara itu, laporan OJK (2023) mengungkap bahwa meskipun sejumlah bank telah menyesuaikan kebijakan internalnya pasca diberlakukannya UU PDP, penerapannya masih cenderung parsial dan terfokus pada aspek teknologi informasi, belum menyatu dengan sistem manajemen risiko dan pengendalian internal secara menyeluruh. COSO (2013) menjadi kerangka yang mampu menjembatani kesenjangan antara aspek hukum dan manajerial melalui lima komponennya, sedangkan DPR RI (2022) memberikan dasar hukum yang memperkuat prinsip *accountability*, *consent*, dan *purpose limitation* dalam pengelolaan data pribadi. Secara keseluruhan, literatur tersebut menegaskan bahwa penerapan COSO tidak hanya penting untuk memperkuat tata kelola dan mitigasi risiko keuangan, tetapi juga berfungsi sebagai instrumen strategis dalam memastikan kepatuhan menyeluruh terhadap UU PDP melalui sinergi antara etika organisasi, pemanfaatan teknologi, dan kesadaran manusia dalam sistem pengendalian internal perbankan Indonesia.

Tabel 2. Analisis Komponen COSO terhadap Kepatuhan UU PDP

Komponen COSO (2013)	**Deskripsi Penerapan di Sektor Perbankan**	**Keterkaitan dengan UU PDP**	**Efek terhadap Kepatuhan**
Control Environment	Membangun budaya integritas dan kepemimpinan yang beretika.	Prinsip akuntabilitas data dan etika perlindungan informasi.	Meningkatkan komitmen manajemen terhadap keamanan data.
Risk Assessment	Mengidentifikasi potensi risiko data (phishing, kebocoran, kesalahan akses).	Analisis risiko data pribadi dan *data breach management*.	Mengurangi potensi pelanggaran hukum.
Control Activities	Menetapkan kontrol akses, otorisasi berlapis, dan audit trail.	Proses pengendalian pemrosesan dan penyimpanan data pribadi.	Memastikan integritas sistem keamanan.
Information & Communication	Menyediakan mekanisme pelaporan dan komunikasi antar unit.	Transparansi dan pelaporan insiden data kepada regulator.	Mempercepat respon insiden dan mitigasi risiko.
Monitoring Activities	Audit internal dan penilaian berkala terhadap efektivitas kontrol.	Kewajiban pelaporan dan pembuktian kepatuhan kepada OJK dan Kemenkominfo.	Menjamin perbaikan berkelanjutan.

(OJK, 2023)	Laporan Kepatuhan Perbankan	Implementasi PDP di bank masih parsial dan berfokus pada TI, belum terintegrasi di manajemen risiko.	Menggambarkan konteks empiris perbankan.

Analisis penerapan komponen COSO terhadap kepatuhan UU Perlindungan Data Pribadi (UU PDP) menunjukkan bahwa setiap elemen kerangka COSO memiliki kontribusi langsung dalam memperkuat tata kelola data di sektor perbankan. Komponen *Control Environment* berperan penting dalam membangun budaya etika dan integritas manajemen yang mendukung prinsip akuntabilitas dan tanggung jawab pengelolaan data pribadi. *Risk Assessment* memastikan bahwa potensi ancaman seperti kebocoran, phishing, dan kesalahan akses dapat diidentifikasi secara sistematis sehingga bank mampu mengembangkan strategi mitigasi yang sesuai dengan ketentuan UU PDP. Melalui *Control Activities*, lembaga perbankan menerapkan kontrol otorisasi berlapis dan audit trail untuk menjamin keamanan serta integritas data nasabah. Selanjutnya, *Information & Communication* memungkinkan terwujudnya transparansi dan pelaporan insiden secara cepat kepada regulator seperti OJK dan Kementerian Kominfo, sedangkan *Monitoring Activities* memastikan adanya audit internal berkala untuk menilai efektivitas pengendalian dan menindaklanjuti temuan pelanggaran. Namun, sebagaimana dilaporkan (OJK, 2023), implementasi kepatuhan PDP di banyak bank masih bersifat parsial dan berfokus pada aspek teknologi informasi tanpa integrasi penuh dengan sistem manajemen risiko. Hal ini menegaskan bahwa penerapan kerangka COSO secara komprehensif menjadi kunci untuk mencapai kepatuhan yang berkelanjutan, karena mampu menghubungkan aspek teknologi, tata kelola, dan perilaku organisasi dalam satu sistem pengendalian yang holistik.



Gambar 1. Model Konseptual Hubungan Variabel Penelitian

Berdasarkan Model Konseptual Hubungan Variabel Penelitian di atas, penelitian ini mengkaji bagaimana efektivitas Sistem Pengendalian Internal (SPI) yang berbasis kerangka COSO (X) memengaruhi Kepatuhan terhadap UU PDP di Sektor Perbankan (Y). Namun, hubungan ini tidak bersifat langsung, melainkan dimoderasi oleh Kesiapan & Kesadaran SDM (Z). Ini berarti bahwa tingkat kesiapan dan kesadaran karyawan memiliki peran krusial dalam menentukan seberapa efektif SPI berbasis COSO dapat diimplementasikan dan pada akhirnya, seberapa baik Perbankan mematuhi regulasi UU PDP. Dengan kata lain, meskipun SPI yang kuat telah dibangun, tanpa SDM yang siap dan sadar,

kepatuhan terhadap UU PDP mungkin tidak akan tercapai secara optimal.

Secara teoretis, hasil penelitian ini menegaskan bahwa efektivitas sistem pengendalian internal berbasis COSO tidak semata bergantung pada struktur dan prosedur formal organisasi, tetapi juga sangat dipengaruhi oleh perilaku dan kesadaran manusia yang mengoperasikannya. Temuan ini memperluas pandangan klasik COSO yang sebelumnya berfokus pada keandalan pelaporan keuangan, menjadi sebuah kerangka pengendalian menyeluruh (*holistic compliance system*) yang mencakup dimensi teknologi, hukum, dan etika organisasi. Integrasi antara kerangka COSO dan prinsip perlindungan data pribadi sebagaimana diatur dalam UU PDP menunjukkan bahwa tata kelola risiko modern menuntut keseimbangan antara mekanisme kontrol struktural dan budaya kesadaran kepatuhan di tingkat individu. Dengan demikian, teori COSO dapat dipandang sebagai sistem dinamis yang tidak hanya menjamin efektivitas internal control, tetapi juga menciptakan perilaku organisasi yang berorientasi pada keamanan dan integritas data.

Secara praktis, penelitian ini memberikan implikasi penting bagi pihak-pihak yang terlibat dalam pengelolaan dan pengawasan sistem perbankan. Bagi Perbankan, hasil penelitian merekomendasikan perlunya peningkatan kapasitas sumber daya manusia melalui pelatihan berkelanjutan mengenai prinsip perlindungan data pribadi (PDP) dan etika digital, guna memperkuat kesadaran dan kompetensi karyawan dalam menjalankan kontrol keamanan informasi. Selain itu, bank perlu mengintegrasikan fungsi risiko, kepatuhan, dan teknologi informasi dalam satu sistem pengendalian internal terpadu agar koordinasi dan pertukaran informasi antarunit menjadi lebih efektif. Langkah penting lainnya adalah melakukan audit kepatuhan PDP secara rutin setidaknya dua kali dalam setahun untuk menilai efektivitas kebijakan, mendeteksi potensi pelanggaran, dan memastikan keberlanjutan kepatuhan terhadap UU PDP.

Bagi Regulator, seperti Otoritas Jasa Keuangan (OJK) dan Kementerian Komunikasi dan Informatika (Kemenkominfo), penelitian ini mendorong upaya harmonisasi antara pengawasan kepatuhan data pribadi dan manajemen risiko teknologi informasi di sektor perbankan. Regulasi yang lebih terintegrasi akan membantu bank menyesuaikan mekanisme kontrol internal sesuai karakteristik risiko digital. Selain itu, regulator disarankan untuk menyediakan panduan teknis yang menggabungkan kerangka COSO dengan COBIT 2019, sehingga tata kelola data pribadi dapat diimplementasikan secara efisien dengan dukungan infrastruktur TI yang memadai.

Dari sisi akademik, penelitian ini membuka peluang bagi pengembangan model pengukuran kuantitatif (*quantitative measurement model*) untuk menilai efektivitas COSO dalam konteks perlindungan data pribadi. Variabel kesadaran dan kompetensi SDM dapat dijadikan variabel moderator empiris yang menggambarkan sejauh mana faktor manusia memediasi hubungan antara sistem pengendalian internal dan tingkat kepatuhan organisasi. Kajian semacam ini akan memperkaya literatur manajemen risiko dan tata kelola data di era digital yang semakin kompleks.

4. KESIMPULAN

Berdasarkan hasil analisis dan pembahasan, dapat disimpulkan bahwa efektivitas sistem pengendalian internal berbasis COSO (Committee of Sponsoring Organizations of the Treadway Commission) memainkan peran sentral dalam menjamin kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) di sektor perbankan Indonesia. Kerangka COSO yang mencakup lima komponen utama yaitu Control Environment, Risk Assessment, Control Activities, Information & Communication, dan Monitoring Activities dalam membentuk fondasi sistemik bagi bank dalam mencegah, mendeteksi, serta menanggulangi potensi pelanggaran data pribadi.

Namun, hasil penelitian menunjukkan bahwa struktur COSO yang kuat saja tidak cukup untuk mencapai kepatuhan substantif terhadap UU PDP. Efektivitasnya sangat bergantung pada kesiapan dan kesadaran sumber daya manusia (SDM) yang mengoperasikan sistem tersebut. SDM dengan tingkat pemahaman tinggi terhadap prinsip privasi, keamanan informasi, dan tanggung jawab etis terbukti mampu mengoptimalkan fungsi pengendalian internal dalam menjaga integritas data nasabah.

Secara konseptual, penerapan COSO dalam konteks UU PDP tidak hanya berfungsi sebagai alat pengendalian risiko finansial, tetapi juga telah berevolusi menjadi kerangka tata kelola kepatuhan yang holistik (holistic compliance framework) yang mencakup aspek hukum, teknologi, dan perilaku organisasi. Oleh karena itu, sinergi antara komitmen manajemen puncak, kompetensi teknis SDM, serta sistem audit dan monitoring yang berkelanjutan menjadi kunci keberhasilan perbankan Indonesia dalam mewujudkan tata kelola perlindungan data yang berintegritas dan berkelanjutan.

Walaupun penelitian ini memberikan gambaran konseptual yang komprehensif mengenai hubungan antara sistem pengendalian internal berbasis COSO, kesadaran SDM, dan kepatuhan terhadap UU PDP, terdapat beberapa keterbatasan yang perlu diperhatikan. Pertama, penelitian ini sepenuhnya menggunakan pendekatan studi literatur sehingga tidak melibatkan data empiris langsung dari perbankan Indonesia, khususnya Bank DKI, sehingga tingkat generalisasi temuan bergantung pada kualitas dan relevansi literatur yang dianalisis. Kedua, sebagian besar referensi internasional berasal dari konteks regulasi negara maju, sehingga terdapat kemungkinan perbedaan dalam penerapan tata kelola data, tingkat literasi digital, serta budaya organisasi dibanding kondisi perbankan domestik. Ketiga, penelitian ini belum mencakup analisis kuantitatif terhadap variabel moderasi seperti kompetensi teknis SDM, efektivitas teknologi keamanan, atau karakteristik risiko ritel, sehingga hubungan antarvariabel masih bersifat konseptual dan belum diuji secara statistik. Keempat, dinamika regulasi privasi data yang terus berkembang, serta perubahan standar keamanan digital, dapat memengaruhi relevansi temuan dalam jangka panjang.

Sarannya Bank DKI perlu melakukan integrasi menyeluruh antara kerangka COSO dan ketentuan UU PDP pada seluruh lini bisnis, termasuk risk management, kepatuhan, pemasaran

kredit, dan divisi operasional. Integrasi ini dapat dilakukan melalui pembaruan SOP, pemetaan ulang siklus pengelolaan data, serta penerapan kontrol akses yang lebih ketat dan berbasis kebutuhan. Kedua, diperlukan program pelatihan berkala yang difokuskan pada tenaga pemasar dan unit risiko ritel, mengingat kelompok ini merupakan pengelola utama data pribadi sensitif dan paling rentan terhadap human error. Pelatihan harus mencakup pengenalan risiko hukum, teknik keamanan dokumen, prosedur komunikasi digital aman, serta prinsip-prinsip dasar UU PDP. Ketiga, instansi perlu mengembangkan mekanisme audit PDP internal, termasuk incident reporting system, early warning system untuk potensi kebocoran data, serta monitoring real-time atas aktivitas transaksi dan akses data. Keempat, Bank DKI disarankan membentuk Data Protection Steering Committee untuk memastikan adanya koordinasi lintas unit dalam menjaga konsistensi penerapan perlindungan data pribadi.

Penelitian selanjutnya disarankan untuk menggunakan pendekatan campuran (mixed methods) agar mampu menangkap baik persepsi pegawai maupun bukti empiris yang lebih kuat terkait tingkat efektivitas penerapan COSO dan kepatuhan terhadap UU PDP. Pengumpulan data dapat diperluas dengan survei terhadap pegawai lini depan, wawancara mendalam dengan pejabat pengelola risiko, serta observasi langsung terhadap alur pengelolaan dokumen nasabah. Selain itu, peneliti selanjutnya dapat menambahkan variabel baru seperti budaya keamanan informasi, kesiapan teknologi (IT readiness), atau model Information Privacy Management (IPM Theory) untuk melihat hubungan yang lebih komprehensif. Penelitian empiris pada berbagai jenis bank baik BUMN, BUMD, bank swasta, maupun BPR juga diperlukan untuk memperoleh gambaran nasional yang lebih representatif. Dengan demikian, temuan penelitian dapat menjadi referensi strategis bagi perbankan Indonesia dalam memperkuat tata kelola perlindungan data pribadi di era digital.

5. DAFTAR PUSTAKA

Ahmed, F., Hussain, A., Khan, S. N., Malik, A. H., Asim, M., Ahmad, S., & El-Affendi, M. (2024). Digital Risk and Financial Inclusion: Balance between Auxiliary Innovation and Protecting Digital Banking Customers. *Risks*, *12*(8). https://doi.org/10.3390/risks12080133

Amoresano, K., & Yankson, B. (2023). Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *HOLISTICA – Journal of Business and Public Administration*, *14*(1), 110–132. https://doi.org/10.2478/hjbpa-2023-0007

Annastasyia Mukrimah Yusuf, Ma'ruf Hafidz, H. K. (2024). Journal of Lex Philosophy (JLP). *Journal of Lex Philosophy (JLP)*, *5*(1), 260–275.

Budiman, R. (2023). The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022. *Jurnal Smart Hukum (JSH)*, *2*(1), 24–36. https://doi.org/10.55299/jsh.v2i1.1352

COSO. (2013). *Internal Control – Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission*.

Dewan Perwakilan Rakyat Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.*

Lembaran Negara RI Tahun 2022 Nomor 182.

Esther, D. (2022). *Common Causes of Data Breaches in Banking and How to Mitigate Them*. *January*.

Kassem, R. (2022). Elucidating corporate governance's impact and role in countering fraud. *Corporate Governance (Bingley)*, *22*(7), 1523–1546. https://doi.org/10.1108/CG-08-2021-0279

Kim, S. D., Andreeva, G., & Rovatsos, M. (2023). *The Double-Edged Sword of Big Data and Information Technology for the Disadvantaged: A Cautionary Tale from Open Banking*. http://arxiv.org/abs/2307.13408

OJK. (2023). *Laporan Tahunan OJK 2023*. jakarta: Otoritas Jasa Keuangan.

Onesti, G., & Palumbo, R. (2023). Tone at the Top for Sustainable Corporate Governance to Prevent Fraud. *Sustainability (Switzerland)*, *15*(3). https://doi.org/10.3390/su15032198

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: a Systematic Literature Review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 226–257. https://doi.org/10.63125/fh49gz18