JURNAL ILMU KOMPUTER
Volume 4 Nomor 1, Januari, 2026
ISSN: 3031-125X (ONLINE)
Penerbit: Program Studi Teknik Informatika S-2 Universitas Pamulang

Perancangan dan Strategi Tata Kelola TI Menggunakan COBIT 2019 pada PT. XYZ

*Iqbal Habib Al Baqi [1], Winarni [2], Taswanda Taryo [3]

[1,2,3)] Teknik Informatika S-2, Program Pascasarjana, Universitas Pamulang, Kota Tangerang Selatan, Banten

Email: iqbalhabib261@gmail.com, dosen02874@unpam.ac.id, dosen02234@unpam.ac.id

ABSTRACT

PT. XYZ faces unstructured and reactive IT governance challenges, characterized by data silos and slow operational application response times. This gap hinders strategic alignment and operational efficiency within an institution that has significant responsibility for public services. This study uses the COBIT 2019 framework to design a systematic and contextual governance strategy. The novelty of this research lies in the holistic integration of the 10 Design Factors in the public sector with a high security risk profile that has not been widely explored. A descriptive qualitative methodology was applied through in-depth interviews, observations, and document studies with key informants from the managerial to operational levels. The analysis follows the COBIT 2019 Design Guide workflow and is validated through triangulation techniques and member checking. The analysis results show a focus on service stability with high security risks (40%) and strict compliance (30%). Of the 40 objectives, 14 priority Governance and Management Objectives (GMO) were identified, focusing on risk optimization and external compliance. The research produced a three-phase strategic roadmap aligned with the organization's objectives and the Personal Data Protection Law regulations. This strategy transforms IT governance at PT. XYZ into a more structured, accountable, and adaptive framework.

Keywords: IT Governance; COBIT 2019; Design Factors; Strategic Roadmap; Information Security.

ABSTRAK

PT. XYZ menghadapi tantangan tata kelola TI yang belum terstruktur dan bersifat reaktif, ditandai dengan adanya silo data serta lambatnya respons aplikasi operasional. Kesenjangan ini menghambat penyelarasan strategis dan efisiensi operasional institusi yang memiliki tanggung jawab signifikan terhadap pelayanan publik. Penelitian ini menggunakan kerangka kerja COBIT 2019 untuk merancang strategi tata kelola yang sistematis dan kontekstual. Kebaruan penelitian terletak pada integrasi holistik 10 Design Factors pada sektor publik dengan profil risiko keamanan tinggi yang belum banyak dieksplorasi. Metodologi kualitatif deskriptif diterapkan melalui wawancara mendalam, observasi, dan studi dokumen dengan informan kunci dari level manajerial hingga operasional. Analisis mengikuti alur kerja COBIT 2019 Design Guide dan divalidasi melalui triangulasi teknik serta member checking. Hasil analisis menunjukkan fokus pada stabilitas layanan dengan risiko keamanan tinggi (40%) dan kepatuhan ketat (30%). Dari 40 objektif, teridentifikasi 14 Governance and Management Objectives (GMO) prioritas yang berfokus pada optimasi risiko dan kepatuhan eksternal. Penelitian menghasilkan peta jalan strategis tiga fase yang selaras dengan tujuan organisasi dan regulasi UU Pelindungan Data Pribadi. Strategi ini mentransformasi tata kelola TI di PT. XYZ menjadi kerangka kerja yang lebih terstruktur, akuntabel, dan adaptif.

Kata kunci: Tata Kelola TI; COBIT 2019; *Design Factors*; Peta Jalan Strategis, Keamanan Informasi.

1. PENDAHULUAN

Dalam era digital yang dinamis, PT. XYZ memegang peranan vital dalam mendukung keamanan dan pelayanan publik melalui pengelolaan data serta sistem

komunikasi yang andal. Namun, efektivitas operasional institusi saat ini terhambat oleh lambatnya respons aplikasi krusial pada jam sibuk dan munculnya silo data akibat pengembangan sistem yang terfragmentasi antar unit. Fenomena ini merupakan indikasi dari pendekatan tata kelola TI yang masih bersifat reaktif dan belum memiliki peta jalan (*roadmap*) jangka panjang yang terstruktur. Tanpa kerangka kerja yang mampu menyelaraskan strategi TI dengan misi organisasi, risiko operasional dan inefisiensi sumber daya akan terus meningkat.

Penelitian terdahulu telah memberikan landasan penting mengenai implementasi COBIT 2019 di sektor publik. Penelitian terdahulu mengidentifikasi bahwa institusi pemerintahan sering kali menghadapi kesenjangan signifikan pada domain kepatuhan dan manajemen risiko [1]. Di sisi lain, penelitian lainnya menekankan bahwa keberhasilan tata kelola sangat bergantung pada integrasi antara sumber daya manusia, proses, dan teknologi untuk menutup celah kapabilitas layanan [2]. Meskipun studi tersebut memberikan wawasan berharga, mayoritas literatur masih berfokus pada audit teknis parsial atau implementasi pada institusi administratif umum. Terdapat celah analisis (*gap analysis*) yang nyata dalam penerapan kerangka kerja tata kelola yang komprehensif pada institusi dengan profil risiko keamanan tinggi dan struktur hierarki yang kompleks seperti PT. XYZ. Studi lain yang relevan mencakup evaluasi kapabilitas di lingkungan sekretariat kabinet, perancangan tata kelola pada pusat data kementerian, institusi pemerintah lainnya, serta rekomendasi tata kelola keamanan informasi di lingkungan kepolisian [3], [4], [5], [6].

Kebaruan (*novelty*) dari penelitian ini terletak pada penggunaan secara holistik 10 *Design Factors* COBIT 2019 untuk merancang sistem tata kelola yang dikustomisasi khusus bagi sektor keamanan publik—sebuah konteks yang belum banyak dieksplorasi dalam riset sebelumnya. Berbeda dengan pendekatan audit standar, penelitian ini memanfaatkan COBIT 2019 sebagai *design toolkit* untuk menghasilkan rekomendasi strategis yang kontekstual. Tujuan dari penelitian ini adalah untuk menganalisis kondisi tata kelola TI saat ini, menentukan prioritas *Governance and Management Objectives* (GMO) berdasarkan profil risiko dan strategi organisasi, serta merumuskan peta jalan strategis yang aplikatif guna menjawab tantangan operasional di PT. XYZ. Manuskrip ini

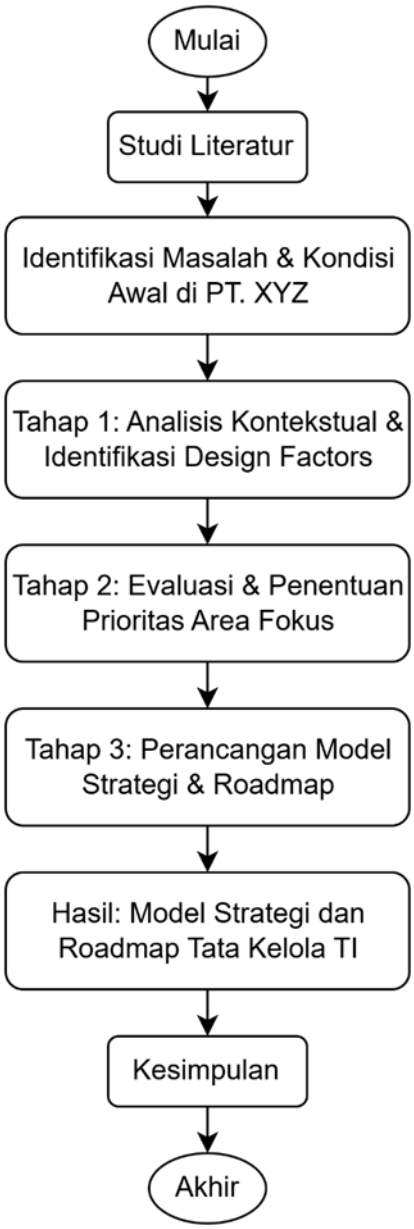
merupakan hasil original dari riset yang dilakukan peneliti untuk memberikan kontribusi praktis bagi penguatan tata kelola TI di sektor publik.

2. METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang berlokasi di PT. XYZ. Informan kunci dipilih menggunakan teknik *purposive sampling* yang mencakup pemangku kepentingan tingkat manajerial hingga operasional teknis guna mendapatkan data yang kaya dan mendalam. Pengumpulan data dilakukan melalui triangulasi teknik yang meliputi wawancara mendalam, observasi langsung terhadap proses kerja, serta studi dokumen internal seperti rencana strategis dan kebijakan TI .

Tahapan penelitian mengikuti alur kerja *COBIT 2019 Design Guide* yang terdiri dari empat fase utama [7]. Pertama, memahami konteks dan strategi organisasi. Kedua, menentukan lingkup awal sistem tata kelola. Ketiga, memperhalus lingkup sistem tata kelola melalui penilaian terhadap 10 *Design Factors*. Keempat, menyelesaikan perancangan sistem tata kelola dengan menetapkan area fokus prioritas. Keabsahan data diuji melalui kriteria kredibilitas menggunakan triangulasi dan *member checking* untuk memastikan interpretasi peneliti sesuai dengan realitas di lapangan.

Tahapan penelitian dirancang secara sistematis sebagaimana divisualisasikan dalam Gambar 1. Alur ini dimulai dari identifikasi masalah empiris, analisis kontekstual, hingga perancangan peta jalan strategis.



Gambar 1. Perancangan Penelitian

Teknik analisis dilakukan terhadap data primer yang bersumber dari transkrip wawancara mendalam dengan informan kunci serta catatan observasi lapangan, serta data sekunder yang berasal dari studi dokumen internal seperti Rencana Strategis dan kebijakan TI PT. XYZ. Data tersebut diolah menggunakan pendekatan kualitatif-interaktif melalui tahapan reduksi data untuk memilah informasi yang relevan dengan faktor desain, penyajian data dalam bentuk matriks atau narasi deskriptif, serta penarikan kesimpulan untuk menentukan prioritas objektif. Proses perancangan sistem tata kelola

secara spesifik mengikuti alur kerja *COBIT 2019 Design Guide* melalui empat fase utama: (1) pemahaman strategi dan konteks organisasi; (2) penentuan lingkup awal sistem tata kelola; (3) pemurnian lingkup melalui penilaian 10 *Design Factors*; dan (4) penyelesaian rancangan sistem tata kelola.

Untuk menjamin kualitas hasil analisis, dilakukan uji keabsahan data yang meliputi uji kredibilitas melalui triangulasi teknik dan *member checking*, pengujian keteralihan melalui deskripsi hasil yang sistematis, serta pengujian ketergantungan melalui *audit trail* terhadap seluruh proses penelitian.

3. HASIL DAN PEMBAHASAN

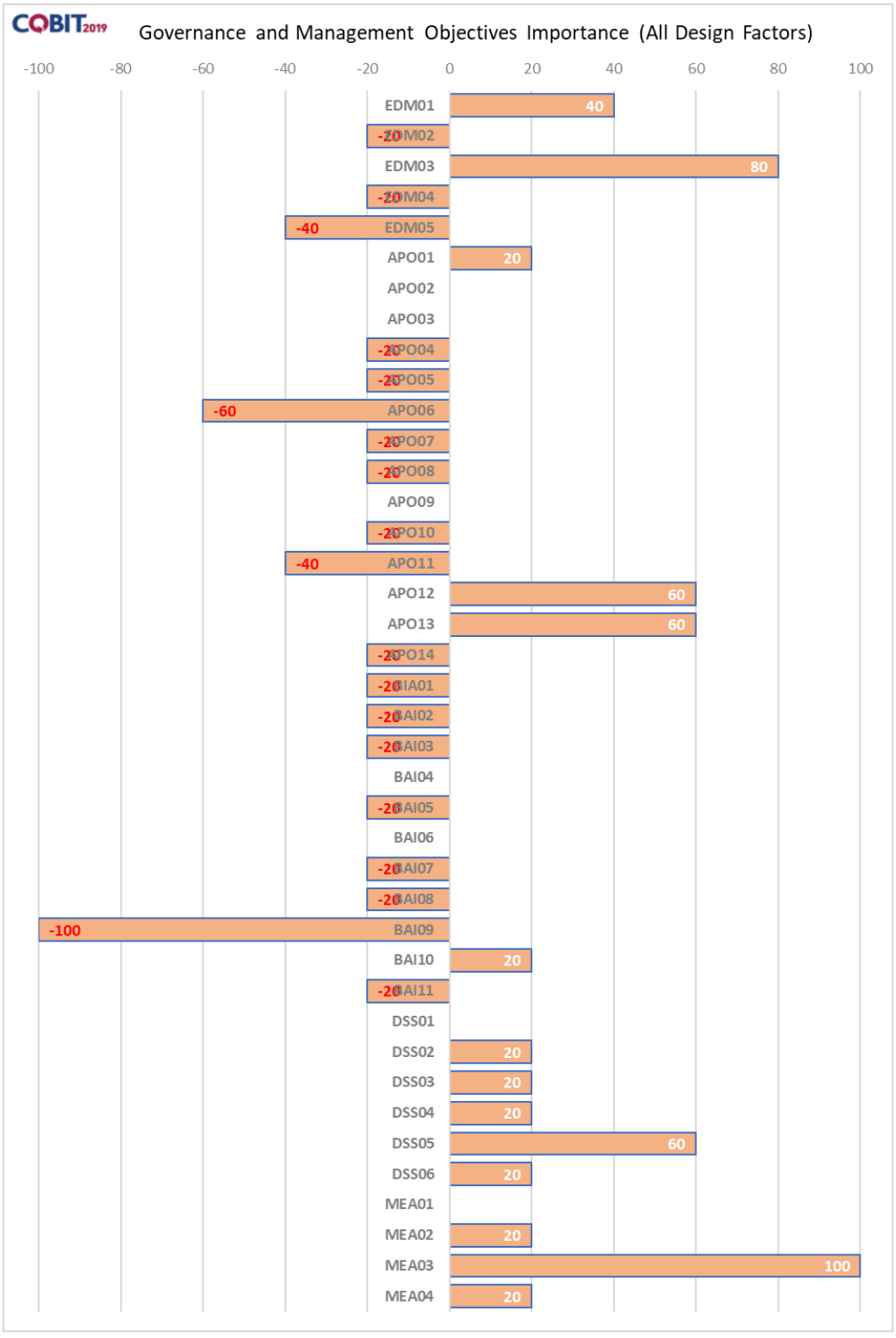
Bagian ini membedah fakta temuan di lapangan yang dikonstruksikan secara logis untuk menjawab tujuan penelitian mengenai perancangan strategi tata kelola TI di PT. XYZ.

3.1. Hasil Analisis *Design Factors* dan GMO

Hasil penilaian terhadap 10 *Design Factors* menunjukkan bahwa PT. XYZ berada pada lingkungan operasional yang sangat mementingkan stabilitas layanan (*Client Service/Stability*) dengan ketergantungan sistem yang masuk dalam kategori *factory* . Kondisi ini didorong oleh peran strategis institusi dalam pelayanan publik yang mengharuskan sistem tersedia 24 jam sehari dan 7 hari seminggu. Profil risiko organisasi menunjukkan kerentanan kritis pada skenario serangan logis dan pengelolaan data, di mana berdasarkan hasil pengolahan pada *COBIT 2019 Design Toolkit*, lanskap ancaman (*threat landscape*) dinilai berada pada tingkat tinggi dengan skor bobot sebesar 40%. Angka tersebut merepresentasikan persepsi risiko terhadap data sensitif yang dikelola institusi dibandingkan dengan lingkungan operasional normal.

Selain itu, distribusi strategi sumber daya pada *Design Factor* 8 menunjukkan dominasi model *insourcing* sebesar 70%, yang berarti mayoritas pengelolaan infrastruktur dan aplikasi dilakukan secara mandiri oleh staf internal. Temuan ini menegaskan bahwa kapabilitas staf internal menjadi penentu utama keberhasilan tata kelola TI, meskipun saat ini masih ditemukan kesenjangan keahlian teknis yang perlu diatasi melalui peta jalan strategis. Pengolahan data melalui *Design Toolkit* tersebut menghasilkan pemetaan tingkat kepentingan untuk 40 objektif COBIT 2019, di mana

teridentifikasi 14 objektif yang memiliki skor kepentingan positif dan menjadi prioritas perbaikan sebagaimana divisualisasikan pada Gambar 2.



Gambar 2. *Governance and Management Objectives* (GMO)

Objektif MEA03 (*Managed Compliance with External Requirements*) menempati prioritas tertinggi dengan skor kepentingan mutlak 100. Skor maksimal ini dihasilkan melalui kalkulasi otomatis pada *toolkit* yang memproses faktor desain strategi organisasi dan kepatuhan, yang mengindikasikan bahwa mandat regulasi seperti UU Pelindungan Data Pribadi (UU PDP) adalah penggerak utama sekaligus kepatuhan wajib bagi perubahan tata kelola di PT. XYZ . Hal ini diikuti oleh EDM03 (*Ensured Risk Optimization*) dengan skor 80, sebuah nilai signifikan yang mencerminkan prioritas manajemen puncak untuk memiliki struktur pengambilan keputusan yang lebih proaktif dan sadar risiko guna menjamin integritas layanan publik.

3.2. Pembahasan dan Strategi Implementasi

Pembahasan hasil menunjukkan adanya hubungan erat antara profil risiko tinggi dengan munculnya domain keamanan (APO12, APO13, DSS05) sebagai area prioritas strategis. Temuan ini menguatkan teori bahwa institusi sektor publik dengan aset data sensitif wajib memprioritaskan optimasi risiko untuk menjaga integritas layanan [6], [8], [9]. Selain itu, tantangan terkait keterbatasan kapasitas SDM internal dan integrasi data yang ditemukan di PT. XYZ selaras dengan hasil penelitian pada sektor publik lainnya [1], [3], [10]. Hal ini menegaskan bahwa keberhasilan tata kelola TI sangat bergantung pada sinkronisasi antara kebijakan regulasi nasional dan kapabilitas sumber daya manusia. Strategi adopsi teknologi yang cenderung sebagai *follower* (70%) menunjukkan sikap hati-hati organisasi dalam meminimalkan kegagalan sistem operasional.

Kesenjangan utama yang ditemukan adalah ketiadaan prosedur tata kelola data terpadu, yang mengakibatkan terjadinya *silo* data dan inefisiensi koordinasi antarunit. Untuk mengatasi hal tersebut, disusun peta jalan strategis tiga fase yang mengintegrasikan penguatan keamanan, integrasi data, dan peningkatan kapasitas SDM internal. Langkah ini selaras dengan penelitian terdahulu yang menekankan bahwa keberhasilan tata kelola TI di sektor publik sangat bergantung pada sinkronisasi antara kebijakan regulasi dan kapabilitas sumber daya manusia [1], [3], [10]. Dengan diterapkannya strategi ini, PT. XYZ dapat mentransformasi pola pengelolaan TI dari reaktif menjadi terstruktur dan akuntabel.

4. KESIMPULAN

Penelitian ini menyimpulkan bahwa kondisi tata kelola TI di PT. XYZ saat ini masih bersifat reaktif dengan kendala utama berupa silo data dan hambatan responsivitas aplikasi operasional. Melalui analisis mendalam terhadap 10 faktor desain COBIT 2019, ditemukan bahwa stabilitas layanan dan profil risiko terhadap serangan logis merupakan faktor yang paling berpengaruh dengan nilai kepentingan maksimal. Berdasarkan fakta tersebut, penelitian berhasil mengidentifikasi 14 objektif tata kelola dan manajemen (GMO) prioritas dari total 40 objektif yang tersedia. Objektif *Managed Compliance with External Requirements* (MEA03) menjadi prioritas tertinggi dengan skor kepentingan mutlak 100 guna memenuhi mandat Undang-Undang Pelindungan Data Pribadi, yang diikuti oleh *Ensured Risk Optimization* (EDM03) dengan skor 80 sebagai upaya transformasi menuju tata kelola yang proaktif.

Strategi yang dihasilkan berupa peta jalan tiga fase memberikan implikasi nyata bagi manajemen untuk memperkuat fondasi keamanan informasi, mengintegrasikan data lintas unit, serta meningkatkan kapabilitas sumber daya manusia internal secara mandiri. Implementasi strategi ini diprediksi dapat meningkatkan akuntabilitas layanan publik dan efisiensi investasi teknologi di institusi keamanan. Model strategi ini juga berpotensi diaplikasikan pada institusi sektor publik lainnya yang memiliki karakteristik profil risiko keamanan tinggi. Sebagai saran untuk pengembangan selanjutnya, peneliti merekomendasikan dilakukannya penilaian tingkat kapabilitas (*capability level*) secara mendalam pada domain keamanan dan kepatuhan yang telah teridentifikasi sebagai prioritas dalam penelitian ini guna mendapatkan hasil perbaikan teknis yang lebih spesifik.

5. DAFTAR PUSTAKA

[1] S. Salimuddin, M. Ula, and N. Nurdin, “ANALISIS KINERJA TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019 PADA UNIVERSITAS JABAL GHAFUR,” *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 2, Apr. 2025, doi: 10.23960/jitet.v13i2.6130.

[2] G. R. Amalia, A. F. Santoso, and D. Praditya, “ANALISIS DAN PERANCANGAN TATA KELOLA TEKNOLOGI INFORMASI PT. XYZ MENGGUNAKAN COBIT 2019 PADA OBJEKTIF BAI01, BAI02, DAN

BAI11," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 2, pp. 578–594, May 2024, doi: 10.29100/jipi.v9i2.4612.

[3] I. W. Budiana, K. Y. E. Aryanto, and I. M. G. Sunarya, "Penilaian Tata Kelola dan Manajemen Infrastruktur TI Bank BPD XYZ Menggunakan COBIT 2019," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 1, pp. 149–161, Jan. 2024, doi: 10.57152/malcom.v4i1.1043.

[4] R. Afdhani and B. Soewito, "Perancangan Tata Kelola TI Menggunakan Framework COBIT 2019 pada Pusat Data dan Informasi Kementerian," *Jurnal Tata Kelola dan Kerangka Kerja TI*, vol. 10, no. 1, p. 22, 2024.

[5] R. Hanafi, M. Munir, S. Suwatno, and C. Furqon, "Identification of IT Governance and Management Objectives and Target Process Capability Level in Government Institution," *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 7, no. 2, pp. 290–308, Aug. 2023, doi: 10.29407/intensif.v7i2.20108.

[6] M. Yasin, A. Akhmad Arman, I. J. M. Edward, and W. Shalannanda, "Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)," in *Proceeding of 14th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/TSSA51342.2020.9310875.

[7] ISACA, *COBIT 2019 Framework Governance and Management Objectives*. 2019.

[8] M. A. Algiffary, M. Izman Herdiansyah, and Y. N. Kunang, "Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI," *JOURNAL OF APPLIED COMPUTER SCIENCE AND TECHNOLOGY (JACOST)*, vol. 4, no. 1, pp. 2723–1453, 2023, doi: 10.52158/jacost.505.

[9] Y. Darmi, S. Fernandez, M. Y. Fathoni, and S. Wijayanto, "Evaluation of Governance in Information Systems Security to Minimize Information Technology Risks," *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 8, no. 1, pp. 40–51, Feb. 2024, doi: 10.29407/intensif.v8i1.21221.

[10] M. D. S. Antariksa, M. P. Angin, and A. P. Widodo, "COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and Benefits Across Various Industry Sectors," *Journal of Renewable Energy, Electrical, and Computer Engineering*, vol. 5, no. 1, pp. 99–105, Mar. 2025, doi: 10.29103/jreece.v5i1.19501.