



PERANCANGAN STRATEGI TATA KELOLA TEKNOLOGI INFORMASI BERBASIS COBIT 2019 UNTUK MENDUKUNG TRANSFORMASI DIGITAL PT XYZ

Bawazir Fadhil Mohammad¹, Basuki Rahmad²

UPN “Veteran” Jawa Timur¹, UPN “Veteran” Jawa Timur²

e-mail : bawazirfadhil@gmail.com

ABSTRACT

Transformasi digital telah menjadi kebutuhan strategis bagi perusahaan industri untuk meningkatkan efisiensi operasional, daya saing, serta kualitas layanan. Namun, implementasi transformasi digital yang tidak diimbangi dengan tata kelola teknologi informasi (TI) yang memadai berpotensi menimbulkan risiko, khususnya terkait keamanan informasi dan pengelolaan risiko siber. PT XYZ sebagai perusahaan manufaktur pupuk nasional menghadapi tantangan dalam menyelaraskan pemanfaatan TI dengan tujuan bisnis perusahaan sekaligus memastikan perlindungan terhadap aset informasi yang semakin kompleks. Oleh karena itu, diperlukan strategi tata kelola TI yang terstruktur, terukur, dan berorientasi pada pengelolaan risiko. Penelitian ini bertujuan untuk merancang strategi tata kelola teknologi informasi berbasis kerangka kerja COBIT 2019 guna mendukung transformasi digital yang aman dan berkelanjutan di PT XYZ. Metode penelitian yang digunakan meliputi studi literatur, pengumpulan data kondisi eksisting tata kelola TI, pemetaan tujuan bisnis terhadap tujuan TI menggunakan mekanisme Goals Cascade, serta analisis faktor desain untuk menentukan domain dan proses COBIT 2019 yang menjadi prioritas. Hasil penelitian menghasilkan rancangan strategi tata kelola TI yang mencakup rekomendasi proses prioritas, penetapan target tingkat kapabilitas, serta peta inisiatif perbaikan tata kelola TI dengan penekanan pada penguatan pengelolaan risiko dan keamanan informasi. Implementasi strategi ini diharapkan mampu meningkatkan keselarasan antara TI dan bisnis, meminimalkan risiko kebocoran data dan ancaman siber, serta mendukung pencapaian tujuan transformasi digital perusahaan secara efektif dan berkelanjutan.

Kata kunci: *Tata Kelola TI, COBIT 2019, Transformasi Digital, Strategi TI, PT XYZ.*

PENDAHULUAN

Perkembangan teknologi informasi (TI) yang pesat telah mendorong organisasi untuk melakukan transformasi digital guna meningkatkan efisiensi operasional, kualitas layanan, serta daya saing di tengah persaingan global. Transformasi digital tidak hanya berkaitan dengan adopsi teknologi baru, tetapi juga menuntut perubahan strategi, proses bisnis, serta tata kelola organisasi agar pemanfaatan TI dapat selaras dengan tujuan bisnis perusahaan. Tanpa tata kelola TI yang baik, investasi teknologi berpotensi tidak memberikan nilai optimal dan bahkan menimbulkan risiko signifikan bagi organisasi, khususnya risiko keamanan informasi dan perlindungan data digital [1].

Dalam beberapa tahun terakhir, meningkatnya insiden kebocoran data, serangan siber, dan penyalahgunaan informasi melalui dark web menjadi tantangan serius bagi organisasi di berbagai sektor industri. Data perusahaan yang berhasil diretas sering kali diperjualbelikan di forum-forum dark web dan dimanfaatkan oleh pihak tidak bertanggung jawab untuk kepentingan finansial, sabotase sistem, maupun pemerasan (ransomware). Kondisi ini menunjukkan bahwa transformasi digital yang tidak diimbangi dengan tata kelola dan pengendalian keamanan TI yang memadai dapat menimbulkan dampak kerugian finansial,



reputasi, serta gangguan operasional yang signifikan.

Sebagai salah satu perusahaan manufaktur pupuk terbesar di Indonesia, PT XYZ memiliki peran strategis dalam mendukung ketahanan pangan nasional. Kompleksitas proses bisnis, skala operasional yang besar, serta tingginya ketergantungan pada sistem informasi terintegrasi menjadikan perusahaan rentan terhadap berbagai ancaman siber, termasuk potensi kebocoran data produksi, keuangan, maupun data strategis perusahaan. Oleh karena itu, selain tuntutan efisiensi dan transparansi, aspek keamanan informasi dan manajemen risiko TI menjadi faktor krusial dalam keberhasilan transformasi digital perusahaan [5].

Seiring dengan upaya PT XYZ dalam menjalankan transformasi digital, diperlukan kerangka tata kelola TI yang tidak hanya berfokus pada penciptaan nilai dan efisiensi, tetapi juga mampu memastikan perlindungan aset informasi, pengendalian risiko keamanan siber, serta kesiapan organisasi dalam menghadapi ancaman eksternal seperti peretasan dan penyalahgunaan data di dark web. Tanpa kerangka tata kelola yang terstruktur, pengelolaan keamanan TI cenderung bersifat reaktif dan tidak terintegrasi dengan strategi bisnis perusahaan.

Tata kelola teknologi informasi berfungsi sebagai mekanisme pengendalian dan pengarah agar TI memberikan nilai tambah bagi organisasi, mengelola risiko secara efektif, serta memastikan kepatuhan terhadap regulasi dan standar yang berlaku, termasuk standar keamanan informasi. Salah satu kerangka kerja yang banyak digunakan secara global dalam tata kelola TI adalah COBIT 2019, yang menyediakan pendekatan komprehensif dan fleksibel dalam merancang [19], mengimplementasikan, serta mengevaluasi tata kelola dan manajemen TI berdasarkan tujuan organisasi, faktor desain, tingkat kapabilitas proses, serta profil risiko, termasuk risiko keamanan informasi.

Namun demikian, penerapan tata kelola TI di banyak organisasi masih menghadapi berbagai tantangan, seperti belum optimalnya keselarasan antara TI dan bisnis, kurangnya fokus pada proses TI yang kritis terkait keamanan data, serta keterbatasan dalam pengukuran kinerja dan kapabilitas pengelolaan risiko siber. Kondisi ini berpotensi meningkatkan celah keamanan yang dapat dimanfaatkan oleh hacker dan pelaku kejahatan siber. Oleh karena itu, PT XYZ memerlukan perancangan strategi tata kelola TI yang sistematis dan terarah agar transformasi digital dapat berjalan secara efektif, aman, dan berkelanjutan.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang strategi tata kelola teknologi informasi berbasis COBIT 2019 yang sesuai dengan kebutuhan dan karakteristik PT XYZ, dengan memperhatikan aspek keselarasan bisnis-TI serta penguatan pengelolaan risiko dan keamanan informasi. Hasil penelitian diharapkan dapat memberikan rekomendasi proses prioritas, target tingkat kapabilitas, serta inisiatif perbaikan tata kelola TI yang mampu mendukung keberhasilan transformasi digital perusahaan sekaligus meminimalkan risiko kebocoran data dan ancaman siber.

METODE PELAKSANAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan studi kasus pada PT XYZ. Pendekatan ini bertujuan untuk memperoleh gambaran menyeluruh mengenai kondisi tata kelola teknologi informasi (TI) yang berjalan serta merancang strategi tata kelola TI yang sesuai untuk mendukung transformasi digital perusahaan. Kerangka kerja COBIT 2019 digunakan sebagai acuan utama dalam proses analisis dan perancangan strategi tata kelola TI.

Tahapan Penelitian

Metode pelaksanaan penelitian ini terdiri dari beberapa tahapan sebagai berikut:



1. Studi Literatur

Tahap awal penelitian dilakukan melalui studi literatur yang bersumber dari buku, jurnal ilmiah, standar, dan dokumen resmi terkait tata kelola TI, transformasi digital, serta kerangka kerja COBIT 2019. Studi literatur bertujuan untuk memperoleh landasan teori dan pemahaman konseptual yang digunakan sebagai dasar analisis dan perancangan strategi tata kelola TI.

2. Pengumpulan Data

Pengumpulan data dilakukan untuk memperoleh informasi mengenai kondisi eksisting tata kelola TI di PT XYZ. Teknik pengumpulan data meliputi:

Wawancara dengan pihak terkait, seperti manajemen TI dan pemangku kepentingan bisnis, untuk menggali kebutuhan, permasalahan, dan harapan terhadap tata kelola TI.

Observasi terhadap proses bisnis dan pengelolaan TI yang berjalan.

Studi dokumen, meliputi kebijakan TI, struktur organisasi, rencana strategis perusahaan, serta dokumen pendukung lainnya.

3. Identifikasi Tujuan Bisnis dan Tujuan TI

Pada tahap ini dilakukan identifikasi dan pemetaan tujuan bisnis perusahaan terhadap tujuan TI menggunakan Goals Cascade COBIT 2019. Pemetaan ini bertujuan untuk memastikan keselarasan antara kebutuhan bisnis dengan dukungan teknologi informasi yang dirancang.

4. Penentuan Faktor Desain COBIT 2019

Penentuan faktor desain (Design Factors) dilakukan untuk menyesuaikan kerangka kerja COBIT 2019 dengan karakteristik dan kebutuhan PT XYZ. Faktor desain yang dianalisis meliputi strategi perusahaan, profil risiko, peran TI, sumber daya TI, serta tingkat

adopsi teknologi. Hasil dari tahap ini digunakan untuk menentukan prioritas domain dan proses COBIT 2019 yang relevan.

5. Penentuan Proses Prioritas COBIT 2019

Berdasarkan hasil pemetaan tujuan dan faktor desain, dilakukan penentuan domain dan proses COBIT 2019 yang menjadi prioritas untuk mendukung transformasi digital perusahaan. Proses-proses terpilih selanjutnya dianalisis untuk menentukan target tingkat kapabilitas yang diharapkan. [20]

6. Perancangan Strategi Tata Kelola TI

Tahap ini menghasilkan rancangan strategi tata kelola TI yang mencakup rekomendasi perbaikan proses, target tingkat kapabilitas, serta inisiatif implementasi tata kelola TI berbasis COBIT 2019. Rancangan strategi disusun agar selaras dengan tujuan bisnis dan mampu mendukung keberhasilan transformasi digital PT XYZ.

7. Penyusunan Rekomendasi

Tahap akhir penelitian adalah penyusunan rekomendasi strategis yang dapat dijadikan acuan oleh perusahaan dalam meningkatkan tata kelola TI secara bertahap dan berkelanjutan. Rekomendasi disajikan dalam bentuk peta inisiatif dan prioritas implementasi.

HASIL DAN PEMBAHASAN

Berdasarkan hasil pengumpulan data dan analisis terhadap dokumen strategis PT XYZ, diperoleh sejumlah tujuan bisnis yang berkaitan langsung dengan pelaksanaan transformasi digital, antara lain peningkatan efisiensi operasional, optimalisasi kualitas layanan, penguatan manajemen risiko, serta peningkatan transparansi dan pengendalian proses bisnis. Tujuan bisnis tersebut kemudian dipetakan ke tujuan tata kelola dan manajemen TI menggunakan mekanisme Goals Cascade pada COBIT 2019. [30]



Hasil pemetaan menunjukkan bahwa tujuan bisnis perusahaan memiliki keterkaitan yang kuat dengan tujuan TI, khususnya dalam aspek penciptaan nilai (value delivery), optimalisasi risiko (risk optimization), dan optimalisasi sumber daya (resource optimization). Hal ini menegaskan pentingnya peran TI sebagai enabler utama dalam mendukung strategi dan keberhasilan transformasi digital perusahaan.

2. Analisis Faktor Desain COBIT 2019

Analisis faktor desain COBIT 2019 dilakukan untuk menyesuaikan penerapan tata kelola TI dengan karakteristik organisasi. Hasil analisis menunjukkan bahwa PT XYZ memiliki strategi bisnis yang berorientasi pada efisiensi, keberlanjutan, dan inovasi digital. Profil risiko perusahaan tergolong menengah hingga tinggi, terutama terkait risiko operasional dan keamanan informasi, mengingat tingginya ketergantungan terhadap sistem informasi dalam proses bisnis inti.

Peran TI dalam organisasi dikategorikan sebagai strategic, di mana TI tidak hanya berfungsi sebagai pendukung operasional, tetapi juga sebagai penggerak inovasi dan peningkatan kinerja bisnis. Berdasarkan faktor desain tersebut, diperlukan fokus pada proses tata kelola dan manajemen TI yang mampu memastikan keandalan sistem, pengelolaan risiko, serta keselarasan TI dengan tujuan bisnis.

3. Penentuan Proses Prioritas COBIT 2019 (Penguatan Aspek Keamanan)

Berdasarkan hasil pemetaan tujuan bisnis, analisis faktor desain, serta profil risiko TI PT XYZ, diperoleh sejumlah proses COBIT 2019 yang menjadi prioritas utama. Selain domain Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), serta Build, Acquire and Implement (BAI), penelitian ini juga menekankan pentingnya proses yang berkaitan langsung dengan keamanan informasi dan pengelolaan risiko siber.

Proses prioritas yang memiliki keterkaitan kuat dengan aspek keamanan data antara lain:

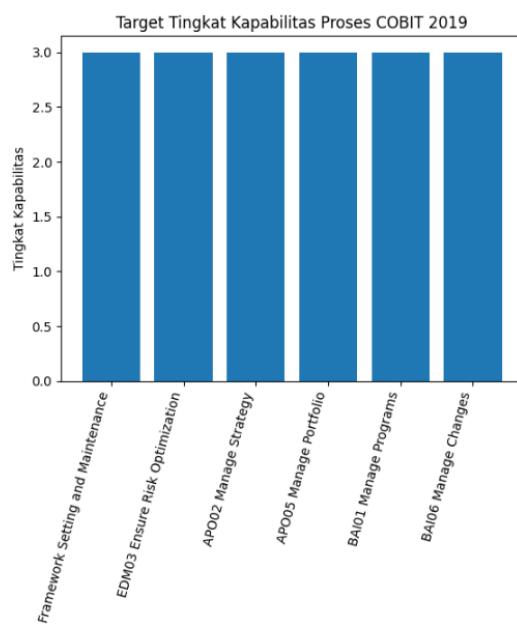
EDM03 (Ensure Risk Optimization), untuk memastikan bahwa risiko TI, termasuk risiko kebocoran data dan serangan siber, dikelola secara optimal dan selaras dengan risk appetite perusahaan.

APO12 (Managed Risk), yang berfokus pada identifikasi, analisis, dan mitigasi risiko TI secara terstruktur.

APO13 (Managed Security), sebagai proses kunci dalam pengelolaan keamanan informasi, perlindungan data, serta pengendalian akses terhadap sistem TI.

DSS05 (Managed Security Services), yang berkaitan dengan implementasi kontrol keamanan operasional, deteksi insiden, serta respons terhadap ancaman siber.

Pemilihan proses-proses tersebut didasarkan pada tingginya ketergantungan PT XYZ terhadap sistem informasi terintegrasi serta meningkatnya ancaman kebocoran data dan serangan siber yang berpotensi dimanfaatkan oleh pihak eksternal melalui dark web. Dengan memprioritaskan proses keamanan ini, tata kelola TI diharapkan mampu memberikan perlindungan yang memadai terhadap aset informasi strategis perusahaan.



Gambar 1. Target Tingkat Kapabilitas Proses Cobit 2019

Penentuan proses prioritas ini bertujuan untuk memfokuskan upaya perbaikan pada area yang memiliki dampak terbesar terhadap penciptaan nilai dan pengelolaan risiko TI, sehingga implementasi tata kelola TI dapat dilakukan secara efektif dan terarah. [33]

4. Penentuan Target Tingkat Kapabilitas Proses (Keamanan Informasi)

Berdasarkan analisis kebutuhan organisasi, target tingkat kapabilitas untuk proses-proses prioritas, termasuk proses keamanan TI, ditetapkan pada level 3 (Established Process). Pada tingkat ini, proses keamanan informasi diharapkan telah:

Terdokumentasi secara formal dalam bentuk kebijakan dan prosedur keamanan TI,
Diterapkan secara konsisten di seluruh unit organisasi,
Didukung oleh mekanisme pengendalian dan pemantauan yang jelas.

Penetapan level 3 dianggap sebagai target yang realistik dan strategis untuk meminimalkan risiko kebocoran data serta meningkatkan kesiapan organisasi dalam menghadapi ancaman hacker dan penyalahgunaan data di dark web. Level ini juga menjadi fondasi penting sebelum organisasi dapat melangkah menuju tingkat kapabilitas yang lebih tinggi,

seperti pengelolaan keamanan berbasis pengukuran dan optimasi berkelanjutan.

5. Rancangan Strategi Tata Kelola TI (Integrasi Keamanan Siber)

Rancangan strategi tata kelola TI berbasis COBIT 2019 yang dihasilkan dalam penelitian ini tidak hanya berfokus pada keselarasan TI dan bisnis, tetapi juga menempatkan keamanan informasi sebagai salah satu pilar utama transformasi digital. Strategi yang dirancang mencakup:

Penyusunan dan penguatan kebijakan keamanan informasi yang selaras dengan tujuan bisnis dan regulasi yang berlaku.

Penetapan struktur peran dan tanggung jawab yang jelas dalam pengelolaan keamanan TI.

Implementasi kontrol keamanan untuk melindungi data perusahaan dari akses tidak sah, kebocoran, dan penyalahgunaan.

Peningkatan kesadaran keamanan (security awareness) bagi sumber daya manusia sebagai bagian dari pengendalian risiko non-teknis.

Selain itu, strategi ini juga dilengkapi dengan peta inisiatif implementasi yang disusun secara bertahap, sehingga penguatan keamanan TI dapat dilakukan secara terencana dan berkelanjutan tanpa mengganggu operasional bisnis utama perusahaan.

6. Pembahasan (Implikasi terhadap Risiko Kebocoran Data)

Hasil penelitian menunjukkan bahwa penggunaan kerangka kerja COBIT 2019 memberikan pendekatan yang sistematis dalam mengintegrasikan tata kelola TI dan pengelolaan keamanan informasi. Pemanfaatan Goals Cascade dan faktor desain memungkinkan organisasi untuk mengidentifikasi proses TI yang paling kritis, termasuk proses yang berperan langsung dalam pencegahan kebocoran data dan mitigasi ancaman siber.

Dengan memfokuskan tata kelola TI pada proses keamanan seperti APO13 dan DSS05, organisasi dapat mengurangi potensi celah keamanan yang sering dimanfaatkan oleh hacker untuk mencuri dan memperdagangkan data perusahaan di dark web. Temuan ini



sejalan dengan penelitian sebelumnya yang menyatakan bahwa tata kelola TI yang kuat berkontribusi signifikan terhadap peningkatan postur keamanan informasi dan ketahanan organisasi terhadap serangan siber. langsung dengan keamanan informasi dan pengelolaan risiko siber.

Proses prioritas yang memiliki keterkaitan kuat dengan aspek keamanan data antara lain: EDM03 (Ensure Risk Optimization), untuk memastikan bahwa risiko TI, termasuk risiko kebocoran data dan serangan siber, dikelola secara optimal dan selaras dengan risk appetite perusahaan.

APO12 (Managed Risk), yang berfokus pada identifikasi, analisis, dan mitigasi risiko TI secara terstruktur.

APO13 (Managed Security), sebagai proses kunci dalam pengelolaan keamanan informasi, perlindungan data, serta pengendalian akses terhadap sistem TI.

DSS05 (Managed Security Services), yang berkaitan dengan implementasi kontrol keamanan operasional, deteksi insiden, serta respons terhadap ancaman siber.

Pemilihan proses-proses tersebut didasarkan pada tingginya ketergantungan PT XYZ terhadap sistem informasi terintegrasi serta meningkatnya ancaman kebocoran data dan serangan siber yang berpotensi dimanfaatkan oleh pihak eksternal melalui dark web. Dengan memprioritaskan proses keamanan ini, tata kelola TI diharapkan mampu memberikan perlindungan yang memadai terhadap aset informasi strategis perusahaan.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa perancangan strategi tata kelola teknologi informasi berbasis COBIT 2019 mampu memberikan pendekatan yang sistematis dan terarah dalam mendukung transformasi digital di PT XYZ, sekaligus memperkuat pengelolaan risiko dan keamanan informasi perusahaan [1].

Hasil penelitian menunjukkan bahwa proses prioritas berada pada domain EDM, APO, BAI, serta DSS, dengan penekanan

khusus pada proses EDM03, APO12, APO13, dan DSS05 yang berkaitan langsung dengan pengelolaan risiko TI dan keamanan data. Target tingkat kapabilitas ditetapkan pada level 3 (Established Process), yang dinilai mampu memberikan fondasi yang kuat dalam meminimalkan risiko kebocoran data dan ancaman siber.

Rancangan strategi tata kelola TI yang dihasilkan mencakup rekomendasi proses prioritas, target kapabilitas, serta peta inisiatif perbaikan yang dapat diimplementasikan secara bertahap. Strategi ini diharapkan tidak hanya meningkatkan efisiensi dan keselarasan TI dengan bisnis, tetapi juga memperkuat perlindungan terhadap aset informasi perusahaan dari potensi serangan hacker dan penyalahgunaan data melalui dark web.

Dengan demikian, penelitian ini dapat dijadikan sebagai acuan bagi PT XYZ dalam memperkuat tata kelola teknologi informasi yang aman, terukur, dan berkelanjutan. Selain itu, hasil penelitian ini juga diharapkan dapat menjadi referensi bagi organisasi lain dengan karakteristik serupa dalam menerapkan tata kelola TI berbasis COBIT 2019 untuk menghadapi tantangan transformasi digital dan ancaman keamanan siber di era digital [6].

DAFTAR PUSTAKA

- [1] ISACA. (2018a). COBIT® 2019 Framework: Introduction and Methodology. ISACA.
- [2] ISACA. (2018b). COBIT® 2019 Framework: Governance and Management Objectives. ISACA.
- [3] ISACA. (2018c). COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution. ISACA.
- [4] ISACA. (2018d). COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution. ISACA.
- [5] ISACA. (2019). COBIT® 2019 Focus Area: Information Security. ISACA.



- [6] ISACA. (2020). COBIT® 2019 Focus Area: DevOps Using COBIT 2019. ISACA.
- [7] Gondodiyoto, S. (2007). *Audit Sistem Informasi: Pendekatan COBIT* (Edisi revisi). Mitra Wacana Media.
- [8] IT Governance Institute (ITGI). (2003). *Board Briefing on IT Governance* (2nd ed.). ITGI.
- [9] IT Governance Institute (ITGI). (2007). *Enterprise Value: Governance of IT Investments*. ITGI.
- [10] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77.
- [11] Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading Digital: Turning Technology into Business Transformation*. Harvard Business Review Press.
- [12] Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business School Press.
- [13] ISO/IEC 38500:2015. (2015). *Information technology—Governance of IT for the organization*. ISO.
- [14] Van Grembergen, W., & De Haes, S. (2009). *Enterprise Governance of IT: Achieving Alignment and Value in Any Organization*. Springer.
- [15] Permana, D. A., Fauzi, R., & Mulyana, R. (2021). Perancangan tata kelola teknologi informasi untuk transformasi digital di industri perbankan menggunakan COBIT 2019. *e-Proceeding of Engineering*, 8(5), 96644.
- [16] Anugerah, M. (2023). Manajemen keamanan informasi untuk transformasi digital berbasis COBIT 2019 Focus Area Information Security. *ZONAsi: Jurnal Sistem Informasi*, 5(3).
- [17] Bayastura, S. F., & Krisdina, S. (2021). Analisis tata kelola teknologi informasi menggunakan framework COBIT 2019 pada PT XYZ. *JIKO (Jurnal Informatika dan Komputer)*.
- [18] Belo, G. I., Atrinawati, L. H., & Wiranti, Y. T. (2020). Perancangan tata kelola teknologi informasi menggunakan COBIT 2019 pada PT Telekomunikasi Indonesia Regional VI Kalimantan. *JUSIKOM*, 4(1), 23–30.
- [19] Dharma, I. G. M. S., Sasmita, G. M. A., & Putra, I. M. S. (2021). Evaluasi dan implementasi tata kelola TI menggunakan COBIT 2019. *Jurnal Ilmiah Teknologi dan Komputer*, 2(2), 354–365.
- [20] Fikri, A. M., et al. (2020). Rancangan tata kelola teknologi informasi menggunakan framework COBIT 2019. *Information Management for Educators and Professionals*, 5(1), 1–14.
- [21] Krismayanti, D., & Sutabri, T. (2023). Analisis IT service management berbasis COBIT 2019. *Jurnal Sistem Informasi*, 5(2), 1–10.
- [22] Nachrowi, E. Y. (2020). Evaluation of governance and management of IT services using COBIT 2019 and ITIL 4. *Jurnal RESTI*, 4(4), 764–774.
- [23] Permatasari, Y., & Haryati, D. (2021). Evaluasi tata kelola TI menggunakan COBIT 2019. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 8(2), 1–8.
- [24] Putra, S. C., & Wijaya, A. F. (2022). Analysis of information technology governance using COBIT 2019. *Journal of Information Systems and Informatics*, 4(4), 1135–1151.
- [25] Sari, R. K., et al. (2023). Perancangan tata kelola teknologi informasi berbasis COBIT 2019. *Jurnal Teknik ITS*, 12(1).
- [26] Syuhada, A. M. (2021). Kajian perbandingan COBIT 5 dan COBIT 2019. *Syntax Literate*, 6(1), 30–39.
- [27] Al-Ma'aitah, M. R. (2021). Digital transformation strategy: A literature review. *Journal of Information Technology and Digital Transformation*, 1(1), 1–15.
- [28] Fitzgerald, M., et al. (2014). Embracing digital: A new strategic imperative. *MIT Sloan Management Review*.



- [29] Hevner, A., et al. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105.
- [30] Merali, Y. (2018). Governance and digital transformation. *Information Systems Frontiers*, 20(3), 565–578.
- [31] Direksi PT XYZ. (2024). *Laporan Tahunan 2023: Strategi Transformasi Digital dan Kinerja Perusahaan*. PT XYZ.
- [32] Humas PT XYZ. (2024, 20 Februari). *XYZ raih penghargaan BUMN terbaik dalam transformasi digital*.
- [33] Wahyudi, B. (2023). *Analisis kebutuhan tata kelola TI untuk mendukung smart factory di PT XYZ*. Skripsi/Tesis.