



Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 1, 106-120
e_ISSN: 2775-0833
<https://jurnalequivalent.id/index.php/jequi/index>
DOI: doi.org/10.59261/jequi.v8i1.264

Pengukuran Kapabilitas Tata Kelola Teknologi Informasi Pada Institusi Keuangan Syariah Menggunakan COBIT 2019

Apririo Kurniajie Kassenda

Universitas Bina Nusantara,
Indonesia

Nilo Legowo

Universitas Bina Nusantara,
Indonesia

***Corresponding author:**

Apririo Kurniajie Kassenda, Universitas Bina Nusantara, Indonesia.

✉ apririo.kassenda@binus.ac.id

Article Info :

Article history:

Received: December 24, 2025

Revised: January 30, 2026

Accepted: February 12, 2026

Keywords:

Information technology governance; COBIT 2019; capability level; gap analysis; CMDB/managed configuration

Kata Kunci:

Tata kelola teknologi informasi; COBIT 2019; tingkat maturitas (capability level); analisis gap; CMDB/konfigurasi terkelola

Abstract

Background: The development of digital banking services increases the reliance of Islamic Financial Institutions on information technology (IT), but also raises the risk of service disruptions, misalignment of technical guidance, and "operational gaps" between high-level provisions and measurable technical implementation. This condition is reinforced by internal findings such as the unavailability of cross-party validated architectural documents and the existence of expired provisions that require updates, so that data-driven IT governance maturity measurement is needed to meet the demands of governance and regulatory compliance.

Objective: This study aims to measure the level of IT governance maturity of Islamic Financial Institutions using the COBIT 2019 framework and identify gaps to prepare measurable improvement recommendations.

Methods: The method used is quantitative descriptive with the stages of determining priority domains through the COBIT 2019 Design Toolkit. A total of seven priority domains were determined as assessment objects, followed by the implementation of Focus Group Discussion (FGD) and filling out the spreadsheet-based COBIT 2019 working paper. The data was analyzed using the COBIT 2019 capability assessment approach including process attribute assessment, capability level determination, and gap mapping to the organization's capability targets.

Results: The measurement results in 7 priority domains showed a variation in achievements: DSS05 and APO01 reached Level 4 (Measured), APO10, BAI09, and APO03 were at Level 3 (Defined), while BAI10 and BAI01 were still at Level 2 (Managed) with the largest gap. These findings confirm the need to strengthen configuration repositories/CMDBs, bind vendor assessment SLAs, standardize project closures and post implementation reviews, and develop user ID control templates for more stable and compliant governance.

Conclusion: In conclusion, COBIT 2019 is effective in mapping the maturity level, uncovering key gaps, and directing priorities for IT governance improvement in Islamic Financial Institutions

Abstrak

Latar belakang: Perkembangan layanan perbankan digital meningkatkan ketergantungan Institusi Keuangan Syariah pada teknologi informasi (TI), namun juga memunculkan risiko gangguan layanan, ketidakselarasan panduan teknis, dan "kesenjangan operasional" antara ketentuan tingkat tinggi dengan implementasi teknis yang terukur. Kondisi ini diperkuat oleh temuan internal seperti belum tersedianya dokumen arsitektur yang tervalidasi lintas pihak serta adanya ketentuan yang kedaluwarsa dan membutuhkan pengkinian, sehingga dibutuhkan pengukuran maturitas tata kelola TI yang berbasis data untuk memenuhi tuntutan tata kelola dan kepatuhan regulator.

Tujuan: Penelitian ini bertujuan mengukur tingkat maturitas tata kelola TI Institusi Keuangan Syariah menggunakan framework COBIT 2019 serta mengidentifikasi gap untuk menyusun rekomendasi perbaikan yang terukur.

Metode: Metode yang digunakan adalah deskriptif kuantitatif dengan tahapan penentuan domain prioritas melalui COBIT 2019 Design Toolkit. Sebanyak tujuh domain prioritas ditetapkan sebagai objek asesmen, dilanjutkan pelaksanaan Focus Group Discussion (FGD) dan pengisian working paper COBIT 2019 berbasis spreadsheet. Data dianalisis menggunakan pendekatan capability assessment COBIT 2019 mencakup penilaian atribut proses, penentuan capability level, pemetaan kesenjangan terhadap target kapabilitas organisasi.

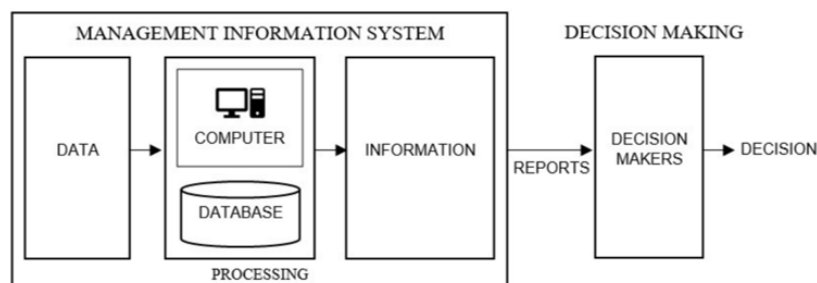
Hasil: Hasil pengukuran pada 7 domain prioritas menunjukkan variasi capaian: DSS05 dan APO01 mencapai Level 4 (Measured), APO10, BAI09, dan APO03 berada pada Level 3 (Defined), sedangkan BAI10 dan BAI01 masih pada Level 2 (Managed) dengan kesenjangan terbesar. Temuan ini menegaskan perlunya penguatan repositori konfigurasi/CMDB, pengikatan SLA penilaian vendor, standarisasi penutupan proyek dan post implementation review, serta penyusunan template kontrol user ID agar tata kelola lebih stabil dan patuh.

Kesimpulan: Kesimpulannya, COBIT 2019 efektif memetakan tingkat maturitas, mengungkap gap utama, dan mengarahkan prioritas perbaikan tata kelola TI pada Institusi Keuangan Syariah

To cite this article: Kassenda, A. K., & Legowo, N. (2026). Pengukuran tingkat kapabilitas tata kelola TI menggunakan COBIT 2019 berbasis design toolkit: Studi kasus Bank XYZ. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(1), 105-117. <https://doi.org/10.59261/jequi.v8i1.264>

PENDAHULUAN

Transformasi digital telah menjadi isu global yang mengubah cara organisasi merancang layanan, mengelola proses bisnis, dan mengambil keputusan berbasis data. Di sektor keuangan, percepatan layanan perbankan digital memperbesar ketergantungan organisasi pada teknologi informasi (TI) sebagai enabler utama layanan end to end, mulai dari operasional internal, keamanan, hingga interaksi nasabah (Putri & Syafruddin, 2023). Strategi transformasi digital yang kuat bukan hanya tentang adopsi teknologi, tetapi juga tentang bagaimana organisasi menyelaraskan tujuan bisnis, kapabilitas TI, dan tata kelola agar perubahan berjalan terarah dan terkendali (Ayu et al., 2022; Hess et al., 2020). Dalam konteks sistem informasi manajemen, keberhasilan adopsi TI juga berkaitan dengan kualitas informasi dan dukungannya terhadap keputusan manajerial (Kiradoo, 2020; Laudon & Laudon, 2004). Dengan demikian, isu global yang relevan dengan penelitian ini adalah kebutuhan organisasi termasuk perbankan untuk memperkuat tata kelola TI (IT governance) agar transformasi digital menghasilkan kinerja layanan yang efektif, aman, dan patuh.



Gambar 1. Komponen MIS dan Pengambilan Keputusan.

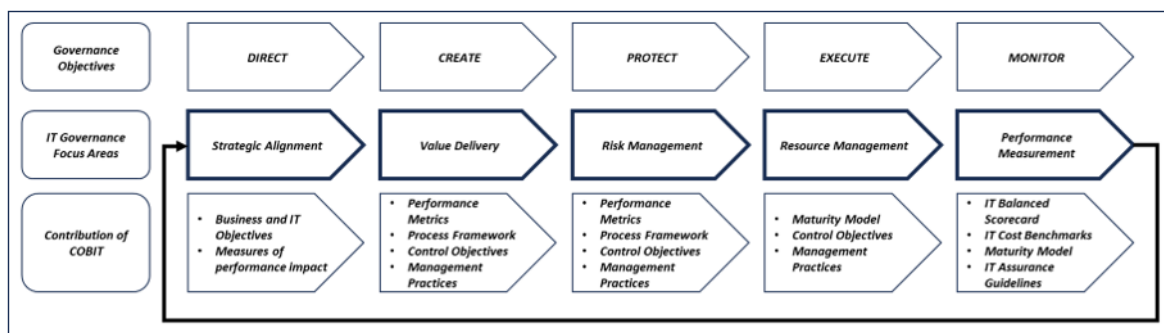
Permasalahan tata kelola TI umumnya tidak muncul secara tunggal, melainkan dipengaruhi oleh kombinasi faktor internal dan eksternal. Pertama, kompleksitas sistem dan integrasi aplikasi meningkat seiring perluasan layanan digital dan perubahan kebutuhan bisnis, yang menuntut pengendalian TI yang lebih disiplin dan terdokumentasi. Kedua, tekanan kepatuhan dan penguatan pengendalian internal semakin kuat karena organisasi harus mengelola risiko operasional, risiko keamanan siber, serta risiko vendor dan pihak ketiga (Adrian & Wang, 2023; Ebert et al., 2020). Ketiga, kesenjangan antara kebijakan tingkat tinggi dan implementasi

teknis sering terjadi ketika standar kerja, dokumentasi arsitektur, pengelolaan konfigurasi, atau mekanisme evaluasi pasca implementasi belum berjalan konsisten (Association, 2018). Keempat, arah transformasi digital yang cepat tanpa penataan governance berpotensi menciptakan keputusan TI yang tidak selaras antar unit, tumpang tindih kontrol, dan lemahnya akuntabilitas.

Dampak dari faktor-faktor tersebut secara langsung mempengaruhi kualitas layanan, keamanan, efisiensi operasional, dan reputasi organisasi (Absari et al., 2024). Ketika tata kelola TI tidak matang, organisasi berisiko mengalami gangguan layanan (downtime), inkonsistensi proses, meningkatnya biaya perbaikan (rework), serta sulitnya memastikan pengendalian internal yang efektif untuk mengurangi risiko teknologi dan keamanan siber (Adrian & Wang, 2023; Ebert et al., 2020). Dari perspektif sistem informasi manajemen, lemahnya kontrol dan kualitas proses TI dapat menurunkan kualitas informasi dan memperlambat pengambilan keputusan, sehingga mengurangi kelincahan organisasi dalam merespons kebutuhan pasar (Kiradoo, 2020; Laudon & Laudon, 2004). Selain itu, pengelolaan vendor dan layanan pihak ketiga yang tidak terukur dapat menimbulkan ketidakpastian kinerja, kegagalan pemenuhan SLA, serta meningkatnya risiko kepatuhan (Turban et al., 2020). Karena itu, penguatan tata kelola TI bukan sekadar kebutuhan teknis, melainkan kebutuhan strategis untuk menjaga keberlanjutan layanan digital dan kepercayaan pemangku kepentingan.

Penelitian ini berfokus pada dua variabel utama, yaitu penerapan framework COBIT 2019 sebagai kerangka tata kelola dan manajemen TI (variabel X) serta tingkat maturitas/kapabilitas tata kelola TI organisasi (variabel Y). IT governance dipahami sebagai mekanisme pengambilan keputusan, struktur akuntabilitas, dan pengendalian yang memastikan TI mendukung tujuan bisnis serta menghasilkan nilai dengan risiko yang terkendali (Ebert et al., 2020; Weill & Ross, 2004). COBIT 2019 menyediakan tujuan tata kelola dan manajemen, praktik, serta pendekatan penilaian kapabilitas yang dapat digunakan untuk memetakan kondisi “as is”, menentukan target “to be”, lalu menyusun langkah perbaikan terukur (Association, 2018; Syuhada, 2021). Sejumlah studi menegaskan COBIT 2019 relevan untuk pengukuran dan perancangan tata kelola TI pada berbagai konteks organisasi, termasuk sektor perbankan dan institusi pendidikan, karena mampu menghubungkan kebutuhan bisnis dengan kontrol TI yang operasional (Siagian et al., 2025; Silaban & Fianty, 2023).

Berbagai penelitian terdahulu menunjukkan bahwa implementasi COBIT 2019 umumnya difokuskan pada desain tata kelola atau penilaian tingkat kapabilitas secara umum, meskipun berbeda dalam fokus domain, konteks organisasi, dan kedalaman rekomendasi (Darmawan & Wijaya, 2022; Fianty & Brian, 2023; Kumape, 2022).



Gambar 2. Siklus Hidup Tata Kelola TI

Pendekatan tersebut cenderung menghasilkan gambaran maturitas yang bersifat komprehensif namun belum tentu langsung berkorelasi dengan akar masalah operasional yang dihadapi organisasi. Dalam konteks sektor perbankan, beberapa studi juga menekankan pentingnya mengaitkan pengukuran kapabilitas dengan penguatan pengendalian internal dan keamanan siber (Andriana et al., 2025), tetapi belum secara eksplisit menempatkan insiden layanan digital sebagai dasar penentuan prioritas domain evaluasi (Adrian & Wang, 2023). Sehingga penelitian ini berupaya mengisi celah praktis tersebut dengan menempatkan insiden operasional sebagai titik awal desain asesmen kapabilitas. Melalui integrasi analisis insiden, pemilihan domain berbasis design toolkit, serta pengukuran capability level COBIT 2019, hasil

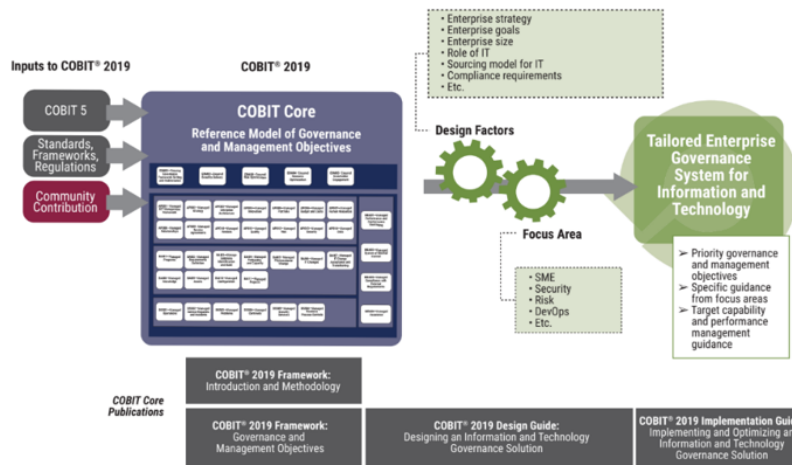
evaluasi tidak hanya memetakan tingkat kapabilitas, tetapi juga dapat langsung diterjemahkan menjadi rekomendasi perbaikan yang spesifik, terukur, dan operasional (Sahara, 2024).

Kebaruan penelitian terletak pada penerapan pendekatan *problem-driven capability assessment*, yaitu pengukuran kapabilitas tata kelola TI yang didahului oleh analisis insiden operasional sebagai dasar penentuan domain prioritas menggunakan COBIT 2019 Design Toolkit. Dengan pendekatan ini, pemilihan domain tidak dilakukan secara normatif atau menyeluruh, melainkan berbasis bukti empiris mengenai area tata kelola yang paling berkontribusi terhadap kesenjangan operasional dan gangguan layanan digital. Hal ini menjadikan proses asesmen lebih kontekstual, terarah, dan relevan dengan kebutuhan organisasi.

Urgensi penelitian ini muncul karena di Institusi Keuangan Syariah menghadapi kebutuhan untuk memastikan bahwa tata kelola TI tidak tertinggal dibanding laju perubahan layanan digital. Di tengah meningkatnya ketergantungan pada TI dan ekspektasi layanan yang selalu tersedia, organisasi perlu memiliki peta kapabilitas yang jelas agar dapat memprioritaskan perbaikan proses yang paling kritis, termasuk penguatan kontrol, kepastian pengelolaan perubahan, pengelolaan vendor, dan evaluasi pasca implementasi (Association, 2018). Tanpa pengukuran maturitas yang sistematis, perbaikan sering bersifat reaktif dan tidak konsisten antar unit, sehingga kesenjangan operasional dapat terus berulang. Di sisi lain, pengukuran kapabilitas yang berbasis *framework* juga membantu organisasi membangun bahasa bersama antara manajemen dan tim teknis dalam mengukur kinerja tata kelola TI secara objektif (Syuhada, 2021; Weill & Ross, 2004). Dengan demikian, penelitian ini mendesak untuk menyediakan dasar pengambilan keputusan perbaikan tata kelola TI yang terstruktur dan dapat dipertanggungjawabkan.

Tujuan penelitian ini adalah mengukur tingkat maturitas/kapabilitas tata kelola TI pada Institusi Keuangan Syariah menggunakan *framework* COBIT 2019, mengidentifikasi kesenjangan (*gap*) antara kondisi saat ini dengan level kapabilitas yang diharapkan, serta merumuskan rekomendasi perbaikan yang relevan pada domain domain prioritas. Penggunaan COBIT 2019 diarahkan untuk menghasilkan gambaran kondisi “*as is*” yang berbasis bukti, sekaligus menyusun arah peningkatan “*to be*” yang realistis dan terukur melalui praktik praktik yang direkomendasikan (ISACA, 2018; Yusuf et al., 2023). Secara konseptual, penelitian ini juga bertujuan memperkuat pemahaman bahwa tata kelola TI merupakan elemen strategis yang berkontribusi pada kualitas layanan digital dan pengendalian risiko (Ebert et al., 2020; Laudon & Laudon, 2004). Dengan tercapainya tujuan tersebut, organisasi memiliki dasar yang lebih kuat untuk mengarahkan program perbaikan tata kelola TI secara prioritatif.

Manfaat penelitian ini diharapkan mencakup manfaat teoritis dan praktis. Secara teoritis, penelitian ini memperkaya literatur mengenai penerapan COBIT 2019 dalam pengukuran kapabilitas tata kelola TI serta menunjukkan keterkaitannya dengan kebutuhan pengendalian internal, efektivitas layanan, dan pengelolaan risiko pada konteks organisasi yang bergantung pada TI (ISACA, 2018; Adrian & Wang, 2023). Secara praktis, hasil penelitian dapat menjadi masukan bagi Institusi Keuangan Syariah dalam menyusun roadmap perbaikan tata kelola TI, menetapkan prioritas penguatan kontrol, dan menstandarisasi proses proses yang masih lemah agar layanan digital lebih stabil dan terukur (Hsing Jung Li et al., 2020; Silaban & Fianty, 2023). Selain itu, penelitian ini juga bermanfaat bagi peneliti dan praktisi sebagai referensi implementasi COBIT 2019 yang lebih operasional, mulai dari pemilihan domain prioritas, pengukuran kapabilitas, hingga penyusunan rekomendasi perbaikan yang dapat langsung ditindaklanjuti (Melissa & Maximillian, 2023; Dewi et al., 2025).



Gambar 3. COBIT Overview

METODE

Penelitian ini menggunakan desain deskriptif kuantitatif dengan pendekatan problem-solving untuk mengukur capability level tata kelola TI serta mengidentifikasi kesenjangan kapabilitas berdasarkan COBIT 2019. Penelitian ini dilakukan pada Institusi Keuangan Syariah sebagai objek studi kasus tata kelola TI, dengan fokus pada proses-proses tata kelola/manajemen TI yang relevan terhadap pengelolaan layanan digital dan pengendalian operasional TI. Pemilihan lokasi dilakukan karena karakter organisasi perbankan menuntut keandalan layanan, kepatuhan, dan pengendalian risiko yang tinggi, sehingga pengukuran kapabilitas tata kelola TI menjadi kebutuhan penting untuk menjaga efektivitas kontrol dan kualitas layanan. Waktu penelitian mengikuti rangkaian tahapan yang tersusun pada Bab Metodologi, mulai dari identifikasi masalah, penentuan domain prioritas dengan design toolkit, FGD, pengukuran tingkat kapabilitas/maturitas, analisis gap, hingga penyusunan rekomendasi. Pendekatan ini sejalan dengan kebutuhan organisasi digital untuk memastikan strategi transformasi berjalan terarah melalui tata kelola dan kontrol yang memadai (Ebert et al., 2020; Hess et al., 2020).



Gambar 4. COBIT Overview

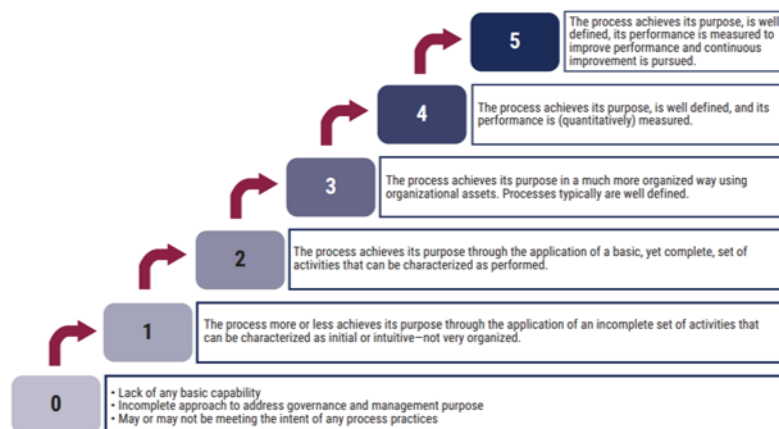
Ruang lingkup penelitian difokuskan pada pengukuran tingkat maturitas/kapabilitas tata kelola TI (variabel Y) dengan mengadopsi COBIT 2019 sebagai kerangka penilaian dan perancangan tata kelola (variabel X). Penelitian menyangkut beberapa aspek utama: (1) penyesuaian (tailoring) sistem tata kelola melalui COBIT 2019 Design Toolkit berbasis design factor, (2) penentuan domain/objektif prioritas yang paling berdampak terhadap kondisi operasional, (3) pengukuran kapabilitas/maturity pada domain prioritas, dan (4) penyusunan

rekomendasi perbaikan yang mengacu pada praktik COBIT dan kebutuhan organisasi. Dalam COBIT 2019, kapabilitas proses dipetakan ke level tertentu untuk menunjukkan seberapa baik proses dikelola dan diukur, sehingga dapat dipakai untuk memandu peningkatan kinerja tata kelola secara bertahap (Association, 2018; Windasari et al., 2022).

Populasi konseptual penelitian ini adalah seluruh pemangku kepentingan internal yang terlibat dalam tata kelola dan manajemen TI di Institusi Keuangan Syariah. Namun, untuk memastikan data yang dikumpulkan relevan dan mendalam, penelitian melibatkan informan kunci melalui forum diskusi terarah dari unit-unit yang memiliki keterkaitan langsung dengan strategi TI, risiko, dan pengendalian operasional. Unit kerja yang dilibatkan meliputi: Unit Kerja Strategi dan Perencanaan IT, Unit Kerja Enterprise Risk Management, Unit Kerja IT Fraud and Risk, serta Unit Kerja IT Senior Operational Risk. Keterlibatan unit-unit tersebut ditujukan untuk memperoleh gambaran lintas fungsi: bagaimana strategi TI diturunkan menjadi kontrol operasional, bagaimana risiko diidentifikasi dan dimitigasi, serta bagaimana kepatuhan dan pengendalian internal dijaga dalam layanan TI perbankan (Adrian & Wang, 2023; Ebert et al., 2020).

Data penelitian dikumpulkan dari dua sumber utama, yaitu: (1) studi dokumentasi dan (2) hasil Focus Group Discussion (FGD). Studi dokumentasi digunakan untuk menilai bukti keberadaan kebijakan, standar, prosedur, catatan aktivitas, serta artefak pengendalian yang berkaitan dengan domain COBIT yang dinilai. Sementara itu, FGD dilaksanakan secara lintas unit kerja yang terkait langsung dengan pengelolaan layanan TI untuk memvalidasi konteks implementasi, mengonfirmasi aktivitas yang benar-benar berjalan, serta menyepakati penilaian atas indikator proses yang dinilai dalam working paper. Pelaksanaan FGD melibatkan perwakilan pemangku kepentingan kunci (process owner, risk management, IT governance, dan operasional TI) dengan jumlah peserta yang disesuaikan dengan struktur organisasi dan cakupan domain prioritas, sehingga penilaian mencerminkan konsensus berbasis pengalaman operasional.

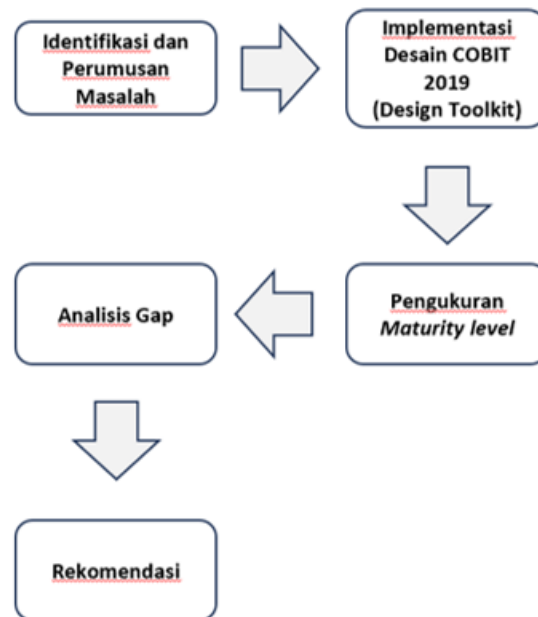
Instrumen kunci penelitian menggunakan COBIT 2019 Design Toolkit untuk menentukan ruang lingkup asesmen dan domain prioritas berbasis faktor desain organisasi, yang menjadi nilai tambah karena memungkinkan pemetaan tata kelola yang lebih kontekstual. Selanjutnya, penilaian kapabilitas dilakukan menggunakan working paper/lembar kerja berbasis spreadsheet yang memuat indikator praktik, aktivitas, dan work product pada setiap proses. Teknik skoring mengacu pada skala pencapaian proses COBIT 2019 (Level 0–5), yaitu Incomplete, Performed, Managed, Defined, Measured, dan Optimizing, dengan penilaian berbasis bukti (evidence-based assessment). Perhitungan level kapabilitas dilakukan secara kuantitatif dengan merata-ratakan skor atribut proses pada setiap level, kemudian dibandingkan dengan ambang batas pencapaian COBIT 2019 untuk menentukan capability level final. Selanjutnya dilakukan analisis gap antara level eksisting dan level target yang ditetapkan organisasi/regulator untuk mengidentifikasi prioritas perbaikan (Association, 2018).



Gambar 5. Capability Level

Tahapan penelitian disusun berurutan agar menghasilkan solusi yang logis dan dapat ditindaklanjuti. Tahap pertama adalah identifikasi dan perumusan masalah, yaitu memetakan indikasi kesenjangan operasional dan kebutuhan penguatan tata kelola TI agar selaras dengan

tuntutan layanan digital dan pengendalian risiko. Tahap kedua adalah implementasi desain COBIT 2019 menggunakan Design Toolkit, yakni menentukan nilai design factor (DF) yang relevan serta menyaring objective/domain prioritas berdasarkan hasil desain agar fokus penilaian tepat sasaran. Tahap ketiga adalah pengukuran maturity/capability level pada domain prioritas melalui FGD dan pengisian working paper untuk menghasilkan level kondisi “as-is”. Tahap keempat adalah analisis gap, yaitu membandingkan capaian “as-is” dengan target yang diharapkan untuk menemukan area yang paling membutuhkan intervensi. Tahap kelima adalah perumusan rekomendasi, yaitu menyusun usulan perbaikan kebijakan/proses/aktivitas kontrol yang langsung menutup gap prioritas dan dapat diintegrasikan ke tata kelola TI Institusi Keuangan Syariah (Association, 2018; Darmawan & Wijaya, 2022; Fianty & Brian, 2023).



Gambar 6. Alur Tahap Penelitian

Analisis dilakukan dengan menggabungkan penilaian kuantitatif (skor/level kapabilitas) dan penjelasan kontekstual hasil FGD serta dokumen pendukung. Secara analitis, setiap domain yang dinilai menghasilkan level kapabilitas/maturity yang menggambarkan kualitas pengelolaan proses, mulai dari pengelolaan yang masih ad-hoc hingga proses yang terukur dan dioptimasi. Untuk menjaga konsistensi penilaian, penelitian mengacu pada konsep tingkat kapabilitas COBIT 2019 yang selaras dengan pendekatan penilaian proses dan peringkat pencapaian aktivitas (misalnya kategori pencapaian yang menggambarkan sejauh mana praktik dijalankan dan dibuktikan). Setelah skor dan bukti terkumpul, gap ditetapkan sebagai dasar prioritas rekomendasi, sehingga kesimpulan penelitian ditarik dari hubungan antara: level kapabilitas yang dicapai, bukti pendukung, serta kebutuhan perbaikan yang paling berdampak terhadap pengendalian layanan TI dan risiko (Syuhada, 2021; Windasari et al., 2022).

HASIL DAN PEMBAHASAN

Hasil

Profil studi penelitian dan konteks kasus Institusi Keuangan Syariah

Penelitian ini mengambil konteks pada Institusi Keuangan Syariah sebagai organisasi perbankan yang tengah berada dalam fase penguatan layanan digital, di mana ketergantungan operasional pada TI menjadi sangat tinggi untuk memastikan layanan berjalan cepat, stabil, dan selalu tersedia. Dalam konteks global, transformasi digital di sektor perbankan menuntut bank tidak hanya berinovasi dari sisi produk, tetapi juga membangun strategi dan tata kelola yang mampu mengarahkan perubahan agar berdampak pada kinerja operasional yang lebih baik. Dengan demikian, fokus studi kasus Institusi Keuangan Syariah ditempatkan pada bagaimana tata kelola TI mampu menutup “kesenjangan operasional” antara ketentuan tingkat tinggi dan

implementasi teknis yang terukur, terutama pasca meningkatnya risiko layanan digital dan tuntutan pengendalian keamanan (Ebert et al., 2020; Hess et al., 2020).

Gambaran spesifik variabel dan objek yang dikaji

Variabel yang dikaji dalam penelitian ini mencakup penggunaan COBIT 2019 sebagai kerangka tata kelola/manajemen TI (variabel X) dan tingkat kapabilitas/maturitas proses tata kelola TI (variabel Y). COBIT 2019 dipilih karena menyediakan pendekatan terstruktur untuk merancang tata kelola berdasarkan konteks organisasi (melalui design factors), memetakan tujuan tata kelola/manajemen, serta menilai kapabilitas proses secara sistematis sehingga hasilnya dapat langsung menjadi dasar rekomendasi perbaikan. Definisi tata kelola TI dalam studi ini merujuk pada mekanisme pengambilan keputusan, struktur akuntabilitas, dan kontrol yang memastikan TI mendukung tujuan bisnis dan menghasilkan nilai dengan risiko yang terkendali (Syuhada, 2021; Weill & Ross, 2004).

Jumlah data yang digunakan dan bentuk bukti (evidence) dalam hasil

Jumlah data kuantitatif operasional yang digunakan dalam hasil mencakup 26 insiden gangguan layanan signifikan pada periode Januari–Desember 2024, yang dicatat dalam data internal Institusi Keuangan Syariah dan menjadi pijakan awal untuk menjelaskan urgensi penguatan tata kelola TI. Selain data insiden, hasil penelitian juga dibangun dari bukti dokumenter (kebijakan, ketentuan, artefak kontrol) dan validasi melalui forum diskusi terarah (FGD) lintas unit sehingga penetapan level kapabilitas tidak hanya berbasis persepsi, tetapi disandarkan pada bukti pelaksanaan kontrol dan konsistensi proses yang berjalan. Pola penggunaan bukti dan validasi lintas pihak ini sejalan dengan praktik penilaian tata kelola TI yang menekankan pentingnya auditabilitas, evidence-based assessment, dan keterukuran kontrol (Adrian & Wang, 2023; Ebert et al., 2020).

Temuan Hasil Operasional (Data Insiden) sebagai Pemicu “Problem-Driven Selection”

Peta insiden layanan TI tahun 2024 dan konsentrasi pada kanal kritikal

Hasil pengolahan data insiden menunjukkan bahwa dari total 26 insiden, konsentrasi gangguan paling dominan berkaitan dengan kanal yang bersentuhan langsung dengan nasabah dan transaksi harian (misalnya kelompok Mobile Banking/SuperApp), diikuti kanal transfer dan sistem pendukung lain. Temuan ini menegaskan bahwa stabilitas layanan digital bukan sekadar isu teknis, melainkan isu tata kelola karena gangguan berulang menandakan adanya ruang perbaikan pada kontrol preventif, standardisasi proses operasional, serta integrasi monitoring dan kontrol. Pada konteks organisasi digital, kualitas tata kelola TI yang baik perlu terhubung dengan penguatan proses layanan TI agar organisasi mampu mempertahankan keunggulan layanan dan respons risiko. (Ebert et al., 2020; Laudon & Laudon, 2004; van der Wulp et al., 2016).

Tabel 1. Ringkasan Insiden Layanan TI Bank XYZ Tahun 2024 (n=26)

Kategori Aplikasi (Ringkas)	Jumlah Insiden	Rata-rata Durasi*	Durasi Min	Durasi Max
Mobile/SuperApp	14	45,64	25	60
BI-Fast	3	39,33	29	45
Core Banking (T24)	2	47,50	45	50
Cash Mgmt (NCMS)	2	37,00	15	59
ATM	1	28,00	28	28
Lainnya (WISE/Visa/Other)	4	bervariasi	28	72

(Sumber: Data Internal Bank XYZ)

*Durasi mengikuti data pada tabel insiden internal (kolom durasi pada naskah) (Ebert et al., 2020; Laudon & Laudon, 2004; Turban et al., 2020).

Implikasi operasional dari insiden terhadap kebutuhan tata kelola TI

Dominasi insiden pada kanal layanan digital menunjukkan bahwa ketahanan (resilience) layanan dan ketepatan kontrol operasional menjadi area prioritas. Secara tata kelola, gangguan berulang sering berkorelasi dengan lemahnya konsistensi pengelolaan perubahan, pengelolaan konfigurasi, serta kesiapan standar pemulihan layanan. Dalam literatur tata kelola TI, kebutuhan

perbaikan seperti ini umum direspons melalui penguatan proses, standardisasi kontrol, dan peningkatan keterukuran kapabilitas agar organisasi tidak terjebak pada pola reaktif. Dengan kata lain, data insiden 2024 berfungsi sebagai bukti “problem-driven” yang memperkuat alasan pemilihan domain COBIT prioritas yang berkaitan dengan keamanan, vendor, aset-konfigurasi, program, arsitektur, serta kerangka manajemen TI (Adrian & Wang, 2023; Ebert et al., 2020).

Hasil Penetapan Ruang Lingkup: Domain Prioritas COBIT 2019 (Output Design Toolkit)

Domain prioritas hasil desain tata kelola (design factor) dan alasan pemilihannya

Berdasarkan proses penyesuaian desain tata kelola menggunakan pendekatan COBIT 2019 (design factors), domain yang diprioritaskan dalam pengukuran kapabilitas dipusatkan pada area yang merefleksikan kebutuhan pasca-risiko siber dan kebutuhan stabilitas operasional.

Tabel 2. Ringkasan Insiden Layanan TI Institusi Keuangan Syariah Tahun 2024 (n=26)

Design Factor		Value
DF1	Enterprise Strategy	Innovation/Differentiation
DF2	Enterprise Goal	Managed Digital Transformations Program
		Product and business innovation
DF3	IT Risk Category	Logical attacks (hacking, malware)
		Unauthorized actions
		Software adoption/usage problems
		IT Operational infrastructure incidents
DF4	IT-Related Issue	Insufficient IT Resources, Staff with Inadequate Skills or Staff Burnout/Dissatisfaction
		Regular issues with data quality and integration of data accross various sources Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT
DF5	Threat Landscape	High
DF6	Compliance Requirements	High
DF7	Role of IT	Strategic
DF8	Sourcing Model for IT	Outsourcing
DF9	IT Implementation Method	Agile
DF10	Technology Adoption	Follower
DF11	Enterprise Size	Large Enterprise

(Sumber: Hasil keputusan FGD pada Institusi Keuangan Syariah)

Domain-domain yang muncul sebagai fokus dan kemudian dinilai meliputi: DSS05 (Managed Security Services), APO10 (Managed Vendors), BAI09 (Managed Assets), BAI10 (Managed Configuration), BAI01 (Managed Programs), APO03 (Managed Enterprise Architecture), dan APO01 (Managed I&T Management Framework). Penetapan ini menegaskan bahwa rancangan tata kelola tidak hanya mengikuti “strategic preference”, tetapi juga menangkap “masalah nyata di lapangan” yang berpotensi menjadi akar gangguan operasional dan kesenjangan kontrol (Darmawan & Wijaya, 2022; Fianty & Brian, 2023).

Hasil studi juga menguatkan adanya beberapa contoh kesenjangan operasional yang sering muncul dalam organisasi: kebijakan sudah ada tetapi belum diterjemahkan menjadi panduan teknis yang jelas, output kontrol tidak terstandarisasi, koordinasi data vendor lintas unit belum terikat SLA, serta belum tersedianya repositori konfigurasi yang andal (misalnya CMDB) untuk memastikan perubahan konfigurasi dapat diverifikasi dan dilacak. Pola kesenjangan seperti ini sejalan dengan literatur tata kelola TI modern yang menekankan pentingnya keterhubungan antara pengendalian internal, keamanan siber, dan kontrol pasca-implementasi agar operasional TI tidak berjalan secara ad-hoc (Adrian & Wang, 2023).

Hasil Pengukuran Capability Level per Domain Prioritas

Hasil pengukuran menunjukkan bahwa Institusi Keuangan Syariah memiliki variasi kematangan pada domain prioritas: terdapat domain yang telah berada pada Level 4 (Measured), sebagian berada pada Level 3 (Defined), dan dua domain masih pada Level 2 (Managed) dengan gap paling besar terhadap target. Target yang digunakan dalam penilaian adalah Level 4 untuk seluruh domain prioritas, sehingga gap dapat dibaca dengan jelas sebagai prioritas perbaikan. Penilaian berbasis level kapabilitas ini konsisten dengan pendekatan COBIT 2019 yang menekankan pengukuran proses sebagai dasar untuk perbaikan bertahap dan terukur (Silaban & Fianty, 2023; Windasari et al., 2022).

Tabel 3. Hasil Capability Level Final dan Target Domain Prioritas COBIT 2019

No	Domain Prioritas	Capability Level Final	Target
1	DSS05 – Layanan Keamanan Terkelola	4	4
2	APO10 – Pemasok Terkelola	3	4
3	BAI09 – Aset Terkelola	3	4
4	BAI10 – Konfigurasi Terkelola	2	4
5	BAI01 – Program Terkelola	2	4
6	APO03 – Arsitektur Terkelola	3	4
7	APO01 – Kerangka Kerja Manajemen TI Terkelola	4	4

(Sumber: Hasil pengolahan penilaian COBIT 2019 pada naskah)

Interpretasi level mengacu pada kerangka kapabilitas COBIT 2019 untuk melihat kualitas pengelolaan proses dan keterukuran kontrol (Syuhada, 2021).

Uraian Temuan per Domain berdasarkan Level Kapabilitas

Pada domain DSS05, hasil menunjukkan bahwa kapabilitas operasional keamanan siber Institusi Keuangan Syariah telah berada pada tingkat terukur (Measured). Secara praktis, capaian ini mengindikasikan proses keamanan seperti pemantauan, deteksi, dan pengelolaan layanan keamanan cenderung sudah berjalan matang dan memiliki keterukuran yang mendukung auditabilitas, sehingga menjadi fondasi penting untuk respons ancaman real-time. Dalam konteks perbankan pasca dinamika ancaman siber, domain keamanan yang kuat merupakan prasyarat untuk menjaga kepercayaan, memastikan kontrol internal efektif, dan mempertahankan layanan digital yang stabil (Adrian & Wang, 2023; Ebert et al., 2020).

Domain APO01 juga mencapai Level 4 yang menandakan bahwa kerangka manajemen TI yang mendasari pengelolaan TI telah memiliki struktur, arah, dan mekanisme yang terukur. Secara tata kelola, kerangka kerja manajemen TI yang matang membantu organisasi memastikan keputusan, kebijakan, dan standar dapat dijalankan secara konsisten lintas unit, sehingga menutup peluang terjadinya “diskoneksi” antara kebijakan dan implementasi. Dalam literatur tata kelola TI, domain kerangka kerja manajemen berperan sebagai pengikat yang memastikan tata kelola tidak hanya reaktif, tetapi terencana dan memiliki mekanisme perbaikan berkelanjutan (Ebert et al., 2020; Weill & Ross, 2004).

Domain APO01 juga mencapai Level 4 yang menandakan bahwa kerangka manajemen TI yang mendasari pengelolaan TI telah memiliki struktur, arah, dan mekanisme yang terukur. Secara tata kelola, kerangka kerja manajemen TI yang matang membantu organisasi memastikan keputusan, kebijakan, dan standar dapat dijalankan secara konsisten lintas unit, sehingga menutup peluang terjadinya “diskoneksi” antara kebijakan dan implementasi. Dalam literatur tata kelola TI, domain kerangka kerja manajemen berperan sebagai pengikat yang memastikan tata kelola tidak hanya reaktif, tetapi terencana dan memiliki mekanisme perbaikan berkelanjutan (Adrian & Wang, 2023; Turban et al., 2020).

Domain APO10 berada pada Level 3 (Defined), yang menunjukkan proses pengelolaan vendor telah didefinisikan dan dijalankan, tetapi belum sepenuhnya terukur dan terintegrasi pada level yang ditargetkan. Pada konteks organisasi yang memiliki ketergantungan signifikan kepada pihak ketiga, gap pada manajemen vendor dapat berimplikasi pada keterlambatan evaluasi, ketidakakuratan basis data vendor, hingga lemahnya pengendalian risiko layanan eksternal. Dalam penelitian tata kelola TI, manajemen vendor yang efektif mensyaratkan standar kinerja,

mekanisme evaluasi, serta alur data yang solid lintas unit agar kontrol dapat berjalan konsisten (Ebert et al., 2020).

Hasil pada BAI09 menunjukkan level defined, yang berarti pengelolaan aset sudah memiliki standar namun belum mencapai keterukuran penuh. Dalam praktik tata kelola TI, aset yang tidak dikelola secara presisi berpotensi memunculkan masalah turunan: inventaris tidak akurat, penelusuran kepemilikan kontrol tidak jelas, serta kesulitan melakukan mitigasi risiko yang bergantung pada akurasi data aset. Karena bank beroperasi pada lingkungan layanan kritikal, penguatan manajemen aset menjadi aspek penting untuk mendukung stabilitas layanan, keamanan, dan kepatuhan (Hess et al., 2020; Laudon & Laudon, 2004).

Domain APO03 juga berada di Level 3 yang menunjukkan adanya definisi dan struktur arsitektur, namun masih memerlukan penguatan keterukuran, validasi lintas pihak, dan mekanisme governance arsitektur agar konsisten menjadi rujukan keputusan teknis. Secara konseptual, arsitektur enterprise yang kuat membantu organisasi menyelaraskan kebutuhan bisnis, standar teknologi, serta arah integrasi sistem sehingga perubahan sistem tidak memunculkan fragmentasi kontrol. Pada konteks transformasi digital, arsitektur yang terkelola sangat berpengaruh dalam mencegah keputusan teknis yang “berjalan sendiri” tanpa rambu tata kelola yang jelas (ISACA, 2018; Laudon & Laudon, 2020; Hess et al., 2016)

BAI10 menjadi domain dengan gap paling kritis, berada pada Level 2 (Managed) dibanding target Level 4. Hal ini menunjukkan proses konfigurasi sudah berjalan dan dikelola pada tingkat tertentu, tetapi belum terstandarisasi menyeluruh dan belum terukur kuat melalui repositori konfigurasi yang andal. Kesenjangan pada konfigurasi sangat relevan terhadap “kesenjangan operasional”, karena tanpa CMDB/konfigurasi baseline yang solid, organisasi akan sulit memverifikasi perubahan yang sah, menelusuri dampak perubahan, dan memastikan integritas layanan. Literatur tata kelola TI juga menekankan bahwa kontrol pasca-implementasi dan pengendalian internal TI sangat bergantung pada kemampuan organisasi menjaga konsistensi data konfigurasi dan bukti perubahan (Ebert et al., 2020).

BAI01 juga masih berada pada Level 2, mengindikasikan pengelolaan program/proyek sudah dilakukan tetapi belum menjadi praktik standar yang terdokumentasi kuat, terutama dalam aspek penutupan program, evaluasi pasca implementasi, dan pengelolaan realisasi manfaat. Kondisi ini relevan dengan kebutuhan organisasi digital karena pelaksanaan proyek yang tidak ditutup secara formal dapat menghambat pembelajaran organisasi, menyulitkan auditabilitas, serta membuat kontrol kualitas implementasi tidak konsisten. Dalam pendekatan problem-solving sistem informasi, penguatan manajemen program penting agar perubahan TI benar-benar menghasilkan manfaat bisnis dan menekan risiko kegagalan operasional (Laudon & Laudon, 2004; Turban et al., 2020).

Secara agregat, hasil menunjukkan pola ketidakseimbangan kapabilitas antara domain strategis dan domain operasional. Domain yang bersifat strategis dan pengendalian makro, seperti DSS05 (Managed Security Services) dan APO01 (Managed I&T Management Framework), telah mencapai Level 4 (Measured), yang menunjukkan adanya proses yang terukur dan terdokumentasi dengan baik. Namun, domain yang berperan langsung dalam pengelolaan perubahan dan stabilitas teknis, yaitu BAI10 (Managed Configuration) dan BAI01 (Managed Programs), masih berada pada Level 2 (Managed). Ketimpangan ini mengindikasikan bahwa meskipun kerangka tata kelola dan kontrol keamanan telah matang, proses operasional yang menjadi penghubung implementasi teknis belum sepenuhnya terstandarisasi dan terukur. Kondisi tersebut berimplikasi pada potensi instabilitas layanan digital, terutama ketika perubahan sistem tidak sepenuhnya didukung oleh baseline konfigurasi dan evaluasi pasca-implementasi yang konsisten (Adrian & Wang, 2023; Ebert et al., 2020)

Perbandingan Final vs Target menunjukkan bahwa gap 1 level (Level 3 → 4) pada APO10, BAI09, dan APO03 dapat diposisikan sebagai “perbaikan penguatan dan keterukuran”, sedangkan gap 2 level (Level 2 → 4) pada BAI10 dan BAI01 adalah “perbaikan struktural” yang berpotensi paling berdampak pada stabilitas layanan. COBIT 2019 mendorong organisasi memprioritaskan domain yang paling memengaruhi tujuan organisasi dan risiko utama, sehingga gap besar pada konfigurasi dan program perlu dipandang sebagai agenda prioritas untuk mengurangi insiden berulang serta meningkatkan kemampuan organisasi dalam pengendalian perubahan dan pemulihan layanan (Silaban & Fianty, 2023).

Pembahasan

Pembahasan ini berangkat dari realitas bahwa transformasi digital dalam industri perbankan bukan lagi sekadar pengembangan kanal layanan, tetapi pergeseran model operasi yang sangat bergantung pada TI sebagai “mesin utama” penyediaan layanan. Dalam kondisi seperti ini, tata kelola TI menjadi pengaman strategis yang memastikan keputusan, kontrol, dan proses TI tetap selaras dengan tujuan bisnis, sekaligus menjaga risiko tetap terkendali. Kerangka tata kelola yang kuat membantu organisasi mengelola hak keputusan TI, menata akuntabilitas, dan menghindari fragmentasi implementasi antar unit. Hal tersebut sejalan dengan pandangan bahwa perusahaan berkinerja tinggi menempatkan IT governance sebagai instrumen untuk memastikan TI benar-benar menghasilkan nilai dan meminimalkan risiko operasional (Ebert et al., 2020; Hess et al., 2020; Weill & Ross, 2004).

Hasil penelitian menunjukkan adanya bukti empiris berupa 26 insiden gangguan layanan signifikan sepanjang Januari–Desember 2024, dengan konsentrasi insiden yang tinggi pada kanal layanan digital/ yang bersentuhan langsung dengan transaksi harian. Data ini tidak sekadar angka, tetapi indikasi kuat bahwa stabilitas layanan belum sepenuhnya ditopang oleh kontrol operasional yang matang dan terukur, terutama pada proses yang bersifat lintas sistem dan lintas unit. Dalam perspektif sistem informasi manajemen, gangguan layanan yang berulang dapat menghambat kualitas informasi, memperlambat respons keputusan, dan menurunkan pengalaman pengguna; sehingga perbaikan harus diarahkan pada penguatan proses inti (governance & control), bukan hanya penanganan insiden secara reaktif (Kiradoo, 2020; Laudon & Laudon, 2004; Turban et al., 2020).

Secara tata kelola, insiden yang berulang umumnya terkait dengan kombinasi faktor: perubahan sistem yang cepat tanpa baseline konfigurasi yang kuat, keterbatasan repositori konfigurasi (misalnya CMDB), proses manajemen program yang belum menutup siklus pembelajaran (post-implementation review), serta pengelolaan vendor yang belum sepenuhnya terukur. Ketika proses konfigurasi belum stabil, organisasi kesulitan memastikan perubahan yang dilakukan dapat dilacak, diverifikasi, dan dinilai dampaknya. Akibatnya, potensi mismatch konfigurasi meningkat dan bisa memicu gangguan layanan. Selain itu, kontrol internal TI pada fase pasca implementasi sistem membutuhkan daftar item kontrol yang jelas untuk memastikan sistem tetap memenuhi standar setelah go-live tanpa penguatan kontrol pasca implementasi, perbaikan cenderung berulang dan tidak menutup akar masalah (Adrian & Wang, 2023).

Hasil pengukuran kapabilitas pada 7 domain prioritas (DSS05, APO01, APO10, BAI09, APO03, BAI10, BAI01) menunjukkan pola yang tegas: dua domain telah mencapai Level 4 (Measured), tiga domain berada pada Level 3 (Defined), dan dua domain tertinggal di Level 2 (Managed). Peta “as-is” ini penting karena menjelaskan bahwa Institusi Keuangan Syariah tidak memulai dari nol ada area yang sudah matang namun ada juga “bottleneck” yang berpotensi menjadi akar ketidakstabilan layanan. COBIT 2019 menempatkan kapabilitas proses sebagai indikator tingkat keterukuran dan konsistensi sehingga gap yang lebih besar mengindikasikan area yang paling membutuhkan intervensi struktural, bukan sekadar perbaikan minor (Silaban & Fianty, 2023; Syuhada, 2021).

Capaian Level 4 pada DSS05 menunjukkan bahwa layanan keamanan terkelola sudah berjalan dengan baik dan terukur, sehingga bank memiliki fondasi kuat dalam monitoring dan pengendalian keamanan. Ini relevan karena sektor perbankan menjadi target ancaman siber yang tinggi, dan efektivitas kontrol internal untuk keamanan siber sangat terkait dengan kematangan tata kelola TI. Di sisi lain, Level 4 pada APO01 menandakan adanya kerangka manajemen TI yang cukup mapan dan terukur yang secara teoritis berperan sebagai “pengikat” agar kebijakan, standar, dan proses dapat diterapkan konsisten lintas unit. Kombinasi keamanan yang terukur dan kerangka manajemen yang matang seharusnya memberi “stabilizer” organisasi namun, hasil tetap menunjukkan gangguan layanan 2024, yang berarti sumber masalah lebih dominan berada pada proses operasional yang memediasi perubahan, konfigurasi, dan implementasi program (Adrian & Wang, 2023; Ebert et al., 2020).

Pada APO10 (Managed Vendors), Level 3 mengindikasikan proses sudah didefinisikan dan dijalankan, tetapi belum sepenuhnya terukur. Dalam konteks bank yang banyak bergantung pada pihak ketiga, vendor governance yang belum terukur berpotensi menimbulkan ketidakpastian SLA, kualitas deliverable, dan koordinasi lintas unit. Pada BAI09 (Managed Assets), Level 3 menandakan manajemen aset sudah berjalan, namun akurasi inventaris, keterlacakan, dan

konsistensi bukti kontrol masih perlu ditingkatkan agar keputusan pengamanan dan perubahan sistem bertumpu pada data aset yang valid. Sementara itu, APO03 (Managed Enterprise Architecture) pada Level 3 menunjukkan arsitektur telah memiliki definisi, tetapi belum sepenuhnya menjadi rujukan terukur dan tervalidasi lintas pihak padahal arsitektur enterprise berfungsi menekan fragmentasi, memastikan integrasi sistem, serta mencegah keputusan teknis yang “berjalan sendiri” tanpa governance. Penguatan pada ketiga domain ini cenderung memberi dampak menengah-besar: memperbaiki keterukuran, memperjelas akuntabilitas, dan menutup celah koordinasi (Laudon & Laudon, 2004; Turban et al., 2020).

Berdasarkan gap yang ditemukan, solusi utama seharusnya diarahkan pada peningkatan kapabilitas proses hingga minimal Level 3 yang solid dan bergerak menuju Level 4 yang terukur. Pada BAI10, solusi strategis mencakup penguatan repositori konfigurasi/CMDB, penetapan baseline konfigurasi yang disepakati, mekanisme audit trail perubahan, dan standardisasi bukti perubahan agar setiap modifikasi dapat diverifikasi serta dievaluasi dampaknya. Pada BAI01, solusi berfokus pada standardisasi penutupan proyek, post-implementation review, dan kerangka pengukuran manfaat agar setiap implementasi menghasilkan pembelajaran dan kontrol residual yang jelas. Pada APO10, penguatan SLA penilaian vendor dan keterpaduan basis data vendor lintas unit akan meningkatkan keterukuran. Sementara pada BAI09, peningkatan akurasi inventaris aset dan linkage dengan kontrol keamanan akan menutup celah risiko operasional. Secara keseluruhan, solusi ini konsisten dengan filosofi COBIT 2019: memperbaiki proses berdasarkan kapabilitas dan bukti, bukan sekadar “program perbaikan” yang tidak terukur (Turban et al., 2020).

Apabila perbaikan dilakukan hingga proses berada pada level terukur, dampak yang diharapkan bersifat berlapis. Pertama, stabilitas layanan meningkat karena kontrol perubahan dan konfigurasi lebih tertib ini akan menurunkan peluang insiden berulang yang berasal dari mismatch konfigurasi atau perubahan yang tidak terdokumentasi. Kedua, efisiensi operasional meningkat karena tim tidak menghabiskan waktu untuk rework atau troubleshooting tanpa baseline yang jelas organisasi lebih cepat melakukan root cause analysis karena bukti kontrol (artefak) tersedia dan terstruktur. Ketiga, dari sisi pengendalian internal dan keamanan siber, proses yang terukur memperkuat auditabilitas dan compliance readiness terutama penting bagi perbankan yang berhadapan dengan tuntutan pengawasan ketat. Dengan kata lain, “Measured” bukan sekadar angka level, tetapi indikator bahwa proses sudah dapat dipantau, dievaluasi, dan ditingkatkan secara konsisten (Silaban & Fianty, 2023).

Jika dibandingkan dengan penelitian terdahulu, kontribusi penelitian ini menjadi lebih jelas. Studi Darmawan & Wijaya (2022) dan Kumape (2022) menekankan analisis/desain tata kelola TI menggunakan COBIT 2019 pada konteks perusahaan, namun konteks, fokus domain, dan penekanan problem-driven (berangkat dari data insiden operasional) tidak selalu menjadi pusat analisis. Studi Melissa & Maximillian (2023) membahas implementasi governance pada perusahaan BPO, yang memberi pembelajaran penting terkait penerapan COBIT 2019, tetapi konteks perbankan memiliki karakter risiko dan kepatuhan yang berbeda sehingga prioritas domain dan dampaknya juga berbeda. Selain itu, studi Silaban & Fianty (2023) menekankan pengukuran capability level, namun penelitian ini menambahkan dimensi “desain prioritas” yang menuntun penilaian pada domain yang paling terkait dengan gap operasional. Dengan demikian, novelty penelitian ini tidak sekadar “mengukur kapabilitas”, tetapi menghubungkan desain prioritas, pengukuran, dan rekomendasi yang langsung menutup gap terbesar pada area yang paling mempengaruhi stabilitas layanan digital (Adrian & Wang, 2023; Ebert et al., 2020).

Literatur tata kelola TI menegaskan bahwa governance perlu menghubungkan tujuan strategis organisasi dengan kontrol dan akuntabilitas yang operasional. COBIT 2019 relevan karena menyediakan tujuan tata kelola/manajemen, mekanisme tailoring melalui design factors, dan pendekatan kapabilitas proses yang dapat dipakai lintas industri. Pada konteks perbankan, temuan Adrian & Wang (2023) menunjukkan keterkaitan langsung antara kapabilitas governance dan efektivitas pengendalian internal untuk keamanan siber hal ini sejalan dengan hasil penelitian yang menunjukkan domain keamanan sudah kuat, namun kontrol operasional (konfigurasi dan program) perlu dikuatkan agar keamanan dan stabilitas saling menopang. Selain itu, Ebert et al. (2020) menegaskan pentingnya IT governance sebagai kerangka kerja untuk memastikan TI dikelola dengan tepat sementara Weill & Ross (2004) menempatkan governance sebagai pengelola hak keputusan TI. Penelitian ini selaras dengan pandangan tersebut, karena

rekomendasi diarahkan pada area yang membuat keputusan dan perubahan TI menjadi lebih tertib, teratur, dan dapat diaudit (Darmawan & Wijaya, 2022; Fianty & Brian, 2023; Kumape, 2022; Silaban & Fianty, 2023).

KESIMPULAN

Penelitian ini menunjukkan bahwa kapabilitas tata kelola TI Institusi Keuangan Syariah tidak homogen: sebagian proses sudah berada pada level teratur dan stabil, sementara beberapa proses inti yang berperan sebagai “penghubung” perubahan layanan khususnya pengelolaan konfigurasi dan pengelolaan program masih tertinggal dibanding target, sehingga berpotensi memperbesar peluang terjadinya gangguan layanan dan inkonsistensi kontrol. Studi ini berkontribusi dengan menguatkan pemanfaatan COBIT 2019 sebagai pendekatan yang tidak hanya melakukan penilaian kapabilitas, tetapi juga menuntun prioritas perbaikan secara kontekstual dan berbasis bukti, sehingga temuan dapat langsung diterjemahkan menjadi agenda penguatan tata kelola TI yang selaras dengan kebutuhan stabilitas layanan digital dan pengendalian risiko. Secara ilmiah, temuan ini menegaskan relevansi perspektif IT governance bahwa nilai TI ditentukan oleh ketepatan keputusan, akuntabilitas, dan keterukuran kontrol lintas proses, bukan semata oleh ketersediaan teknologi. Keterbatasan penelitian ini terletak pada ruang lingkup yang berfokus pada domain prioritas dan ketergantungan pada bukti yang tersedia dari unit terkait pada periode pengukuran, sehingga generalisasi ke organisasi lain perlu dilakukan dengan kehati-hatian. Penelitian selanjutnya disarankan menguji dampak implementasi rekomendasi melalui studi longitudinal (sebelum-sesudah) terhadap indikator kinerja layanan (misalnya tren insiden, durasi pemulihan, kepatuhan kontrol), memperluas cakupan domain untuk melihat keterkaitan antarproses (end-to-end governance), serta mengombinasikan penilaian kapabilitas dengan metrik risiko dan kinerja vendor guna memperoleh peta peningkatan tata kelola TI yang lebih komprehensif.

UCAPAN TERIMA KASIH

Penulis menyampaikan apresiasi dan ucapan terima kasih yang sebesar-besarnya kepada manajemen beserta seluruh jajaran unit kerja di Institusi Keuangan Syariah (Bank XYZ) yang telah memberikan dukungan penuh, kemudahan akses data, serta partisipasi aktif selama proses pengumpulan informasi melalui studi dokumentasi dan Focus Group Discussion (FGD). Dukungan tersebut sangat esensial dalam penyediaan bukti empiris yang menunjang keakuratan pengukuran tingkat kapabilitas tata kelola teknologi informasi pada penelitian ini.

Penulis juga menyampaikan penghargaan yang setinggi-tingginya kepada Universitas Bina Nusantara atas dukungan akademik serta fasilitas lingkungan ilmiah yang kondusif. Akhir kata, terima kasih kepada seluruh pihak yang tidak dapat disebutkan satu per satu, yang telah memberikan masukan, arahan, serta kontribusi pemikiran sehingga penelitian ini dapat diselesaikan secara komprehensif dan sistematis.

PERNYATAAN KONTRIBUSI PENULIS

Apririo Kurniajie Kassenda bertindak sebagai peneliti utama yang berkontribusi dalam konseptualisasi ide penelitian, perancangan metodologi, pelaksanaan asesmen tingkat kapabilitas tata kelola teknologi informasi berbasis COBIT 2019, pengumpulan dan analisis data empiris, serta penulisan draf awal naskah. Nilo Legowo berkontribusi dalam pengembangan kerangka konseptual, validasi metodologi, interpretasi hasil analisis, peninjauan kritis terhadap substansi ilmiah, serta memberikan supervisi akademik secara menyeluruh terhadap keseluruhan proses penelitian. Seluruh penulis telah berpartisipasi aktif dalam proses revisi naskah, membaca dan menyetujui versi akhir artikel yang dipublikasikan, serta bertanggung jawab penuh atas integritas dan keabsahan seluruh substansi penelitian.

DAFTAR PUSTAKA

- Absari, R., Harijanja, T., & Kalbuana, N. (2024). Faktor-Faktor Yang Mempengaruhi Kepuasan Pelanggan Terhadap Pelayanan Pada Bandar Udara: Faktor Kualitas Pelayanan, Fasilitas, Dan Harga Tiket. *Journal of Management and Innovation Entrepreneurship (JMIE)*, 1(4), 692–701.
- Adrian, F. X., & Wang, G. (2023). Measure the level capability IT governance in effectiveness internal control for cyber security using the COBIT 2019 in organization: Banking company.

- Journal of Theoretical and Applied Information Technology*, 15(5), 1710–1723.
- Andriana, D., Firmansyah, G., Tjahjono, B., Widodo, A. M., & Akbar, H. (2025). Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 Pada Rumah Sakit Medika Dramaga. *Jurnal Locus Penelitian Dan Pengabdian*, 4(8), 8303–8318.
- Association, I. S. A. and C. (2018). *COBIT® 2019 Framework: Governance and Management Objectives*. ISACA.
- Ayu, I. W., Zulkarnaen, Z., & Fitriyanto, S. (2022). budaya digital dalam transformasi digital menghadapi era society 5.0. *Jurnal Pengembangan Masyarakat Lokal*, 5(1), 20–25.
- Darmawan, D., & Wijaya, A. F. (2022). Analisis dan Desain Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada PT. XYZ. *Journal of Computer and Information Systems Ampera*, 3(1), 1–17.
- Ebert, C., Vizcaino, A., & Manjavacas, A. (2020). IT governance. *IEEE Software*, 37(6), 13–20.
- Fianty, M. I., & Brian, M. (2023). Leveraging COBIT 2019 framework to implement IT governance in business process outsourcing company. *Journal of Information Systems and Informatics*, 5(2), 568–579. <https://doi.org/10.51519/journalisi.v5i2.492>
- Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2020). Options for formulating a digital transformation strategy. In *Strategic information management* (pp. 151–173). Routledge.
- Kiradoo, G. (2020). A study on management information systems role and adoption in managerial decision making. *International Journal of Management (IJM)*, 11(3).
- Kumape, S. C. A. (2022). Perancangan tata kelola teknologi informasi menggunakan COBIT 2019 pada PT. X. *JATISI*, 9(2), 1568–1580. <https://doi.org/10.35957/jatisi.v9i2.2115>
- Laudon, K. C., & Laudon, J. P. (2004). *Management information systems: Managing the digital firm*. Pearson Educación.
- Putri, C. V., & Syafruddin, M. (2023). Pengaruh Manajemen Risiko Terhadap Kinerja Keuangan Bank (Studi Empiris pada Perusahaan Sektor Keuangan Sub Sektor Bank yang Terdaftar di BEI Tahun 2010–2019). *Diponegoro Journal of Accounting*, 12(2).
- Sahara, E. (2024). *Audit Tata Kelola Teknologi Pada Sistem Informasi E-Learning Universitas Jambi Menggunakan Kerangka Kerja COBIT 2019*. UNIVERSITAS JAMBI.
- Siagian, D. P., Purwandari, B., & Trisnawaty, N. W. (2025). Enhancing Information Technology Maturity with the COBIT 2019 Framework: A Case Study of ABC Univeristy. *The Indonesian Journal of Computer Science*, 14(1). <https://doi.org/10.33022/ijcs.v14i1.4638>
- Silaban, L. R., & Fianty, M. I. (2023). Measurement Of Information Technology Governance Capability Level Using Cobit 2019 Framework. *IJISCS (International Journal of Information System and Computer Science)*, 7(2), 78–88. <https://doi.org/10.56327/ijiscs.v7i2.1543>
- Syuhada, A. M. (2021). Kajian Perbandingan Cobit 5 dengan Cobit 2019 sebagai Framework Audit Tata Kelola Teknologi Informasi. *Syntax Literate; Jurnal Ilmiah Indonesia*, 6(1), 30–39. <https://doi.org/10.36418/syntax-literate.v6i1.2082>
- Turban, E., Pollard, C., Wood, G., & Beynon-Davies, P. (2020). *Business Information Systems: A Problem-Solving Approach*. Pearson.
- Van der Wulp, S. A., Dsikowitzky, L., Hesse, K. J., & Schwarzbauer, J. (2016). Master Plan Jakarta, Indonesia: The Giant Seawall and the need for structural treatment of municipal waste water. *Marine Pollution Bulletin*, 110(2), 686–693.
- Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.
- Windasari, I. P., Rochim, A. F., Alfiani, S. N., & Kamalia, A. (2022). Audit Tata Kelola Teknologi Informasi Domain Monitor, Evaluate, and Asses dan Deliver, Service, Support Berdasarkan Framework COBIT 2019. *J. Sist. Info. Bisnis*, 11(2), 131–138. <https://doi.org/10.21456/vol11iss2pp131-138>