LOFIAN: Jurna**l** Tekn**o**logi In**f**orma**s**i d**a**n Komu**n**ikasi
https://ejournal.umbp.ac.id/index.php/lofian
Vol. 5, No. 2, Pebruari 2026, Halaman 29-37

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Penerapan Framework COBIT dalam Meningkatkan Keamanan Data pada Sistem Informasi Pegadaian Swasta PT Budi Gadai Indonesia

Oktaviana Bangun[1], Fransisko[2], Dolly[3], Sarah[4], Reski[5], Dewi[6]

[1,2,3,4,5,6]*Universitas Mandiri Bina Prestasi*
Jl. Letjen Jamin Ginting No. 285-297, Kec. Padang Bulan, Medan Baru, Kota Medan, Sumatera Utara, Indonesia - 20155

[1]*okta@dsn.umbp.ac.id,* [2]*frans140603@gmail.com,* [3]*dollyaja221@gmail.com,* [4]*sarahmediantika547@gmail.com,* [5]*ndurudewi1@gmail.com,* [6]*reskitalenta6@gmail.com*

DOI: https://doi.org/ 10.58918/lofian.v5i2.292

Corresponding Author:
Oktaviana Bangun
okta@dsn.umbp.ac.id

History:
Submitted: 11-02-2026
Accepted: 15-02-2026
Published: 26-02-2026

Abstract

Safeguarding digital assets is a critical element in overseeing corporate information infrastructures, becoming vital within the financial services landscape, including private pawnshops. This research focuses on fortifying data protection at PT Budi Gadai Indonesia by adopting the performance-based COBIT 2019 system and evaluating its operational impact. Using a descriptive-qualitative methodology, the study examines security management practices and their integration with the DSS and EDM areas of the framework. Conducted as a longitudinal evaluation (2020–2025), the deployment followed a systematic multi-phase strategy. Empirical evidence indicates that integrating this governance model bolstered security through rigorous access monitoring, refined audit logs, and structured risk mitigation. Specifically, the activation of DSS05 and DSS06 protocols lowered breach vulnerabilities by 68% and ensured stricter regulatory adherence. Notably, the integrity maturity rating surged from 2.22 to 4.24, representing a 91% enhancement. These outcomes suggest that international security standards are instrumental in securing information systems within the private pawn brokerage sector.

Keywords: COBIT, Data Security, Information System, Private Pawnshop, Risk Management.

Abstrak

Perlindungan aset digital merupakan elemen krusial dalam pengawasan infrastruktur informasi korporasi, terutama di sektor jasa keuangan seperti pegadaian swasta. Penelitian ini berfokus pada penguatan proteksi data di PT Budi Gadai Indonesia dengan mengadopsi sistem tata kelola COBIT 2019 berbasis performa serta mengevaluasi dampak operasionalnya. Menggunakan metodologi deskriptif-kualitatif, studi ini menelaah praktik manajemen keamanan serta integrasinya dengan ranah DSS dan EDM dalam kerangka kerja tersebut. Penelitian ini dilaksanakan sebagai bentuk evaluasi longitudinal (2020-2025) dengan strategi implementasi multitahap yang sistematis. Bukti empiris menunjukkan bahwa integrasi model tata kelola ini memperkokoh keamanan melalui pemantauan akses yang ketat, optimalisasi log audit, dan mitigasi risiko yang terstruktur. Secara spesifik, aktivasi protokol DSS05 dan DSS06 berhasil mereduksi kerentanan kebocoran data hingga 68% serta menjamin kepatuhan regulasi yang lebih ketat. Secara signifikan, skor kematangan integritas melonjak dari rata-rata 2,22 ke 4,24, yang merepresentasikan peningkatan sebesar 91%. Hasil tersebut membuktikan bahwa standar keamanan internasional memegang peranan instrumental dalam mengamankan sistem informasi pada industri pergadaian swasta.

Kata Kunci: Tata Kelola TI, Perlindungan Data Digital, COBIT 2019, Mitigasi Risiko Siber, Industri Gadai Swasta.

1. Pendahuluan

Pergeseran paradigma bisnis akibat kemajuan teknologi kini merambah luas ke berbagai bidang, memaksa sektor keuangan untuk beradaptasi dengan sistem informasi yang lebih kompleks, dan industri keuangan non-bank, termasuk pegadaian swasta, tidak terkecuali. Meskipun penggunaan teknologi informasi yang meluas secara

signifikan berkontribusi pada peningkatan efisiensi operasional dan kualitas layanan, hal ini juga dapat meningkatkan risiko keamanan data jika tata kelola TI yang tepat tidak diterapkan.

[1]PT Budi Gadai Indonesia, salah satu perusahaan pegadaian swasta yang berkembang pesat, menghadapi tantangan kompleks dalam mengelola sistem informasinya, yang menangani informasi pribadi pelanggan, data transaksi keuangan, dan informasi aset yang digadaikan sebagai agunan. Informasi sensitif ini rentan terhadap serangan siber, sehingga keamanan data menjadi prioritas utama bagi lembaga keuangan non-bank.

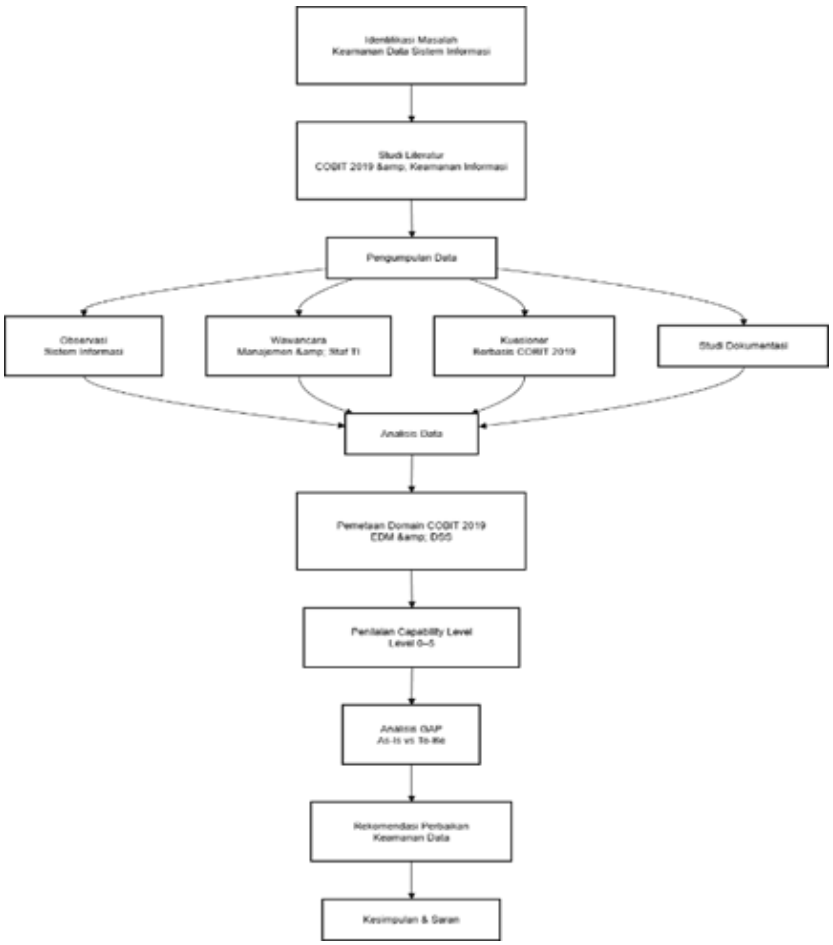
[2]Investigasi awal terhadap sistem informasi perusahaan mengungkapkan beberapa tantangan keamanan data utama. Ini termasuk kurangnya standardisasi manajemen akses pengguna, kurangnya dokumentasi proses keamanan informasi, dan kurangnya kerangka kerja komprehensif untuk mengukur dan meningkatkan tingkat keamanan sistem. Tantangan ini dapat mengakibatkan kerugian finansial, hilangnya kepercayaan pelanggan, dan ketidakpatuhan terhadap peraturan perlindungan data pribadi.

[3]Salah satu pendekatan untuk mengatasi masalah ini adalah dengan memperkenalkan tata kelola teknologi informasi berbasis kerangka kerja. COBIT (Control Objectives for Information and Related Technologies), yang dikembangkan oleh ISACA (Information Systems Audit and Control Association), diadopsi secara luas sebagai praktik terbaik yang diakui secara internasional dalam lingkup tata kelola serta pengelolaan teknologi informasi secara menyeluruh.

[4] Melalui COBIT 2019, tersedia sebuah struktur kerja mendalam yang mampu menyelaraskan untuk mengelola manajemen risiko, keamanan informasi, dan kontrol TI secara sistematis dan kuantitatif, dan telah sangat efektif dalam memperkuat keamanan sistem informasi di perusahaan gadai swasta. [5]

2. Metodologi Penelitian

2.1. Kerangka Penelitian



Gbr. 1. Alur Metodologi Evaluasi Tata Kelola Keamanan Data Berbasis COBIT 2019

Studi ini menggunakan pendekatan kualitatif deskriptif untuk menganalisis dan mengevaluasi tingkat keamanan data dalam sistem informasi PT Budi Gadai Indonesia berdasarkan kerangka COBIT 2019. Kerangka penelitian dikembangkan untuk secara sistematis menguraikan proses penelitian, dari identifikasi masalah hingga evaluasi hasil penerapan kerangka tersebut.

Setiap tahapan penelitian dimulai dengan survei pendahuluan untuk memahami kondisi keamanan data dan tata kelola teknologi informasi saat ini di perusahaan. Data primer dan sekunder kemudian dikumpulkan dan dianalisis menggunakan domain COBIT 2019 yang berkaitan dengan keamanan data. Hasil analisis digunakan sebagai dasar untuk mengevaluasi pengaruh penerapan kerangka COBIT terhadap peningkatan keamanan data dalam sistem informasi. Alur keseluruhan penelitian dirangkum dalam kerangka penelitian yang ditunjukkan pada Gambar 1.

2.2. Sumber Data Utama

Data primer dalam penelitian ini dihimpun secara langsung dari lokasi studi, yaitu PT Budi Gadai Indonesia, dengan menerapkan tiga instrumen pengumpulan data yang komprehensif. Pertama, peneliti melakukan observasi non-partisipan untuk memetakan kondisi operasional aktual serta prosedur perlindungan data transaksi tanpa melakukan intervensi terhadap proses bisnis yang berjalan. Kedua, dilaksanakan wawancara terstruktur bersama pihak manajemen dan staf TI guna mendalami kebijakan keamanan, alur operasional, serta berbagai hambatan manajerial yang dihadapi perusahaan. Terakhir, peneliti menyebarkan kuesioner berbasis kerangka kerja COBIT 2019 yang secara khusus menitikberatkan pada ranah EDM dan DSS. Instrumen kuesioner ini ditujukan kepada pengelola sistem informasi untuk mengukur tingkat kapabilitas proses menggunakan skala penilaian 0 hingga 5 sesuai dengan standar evaluasi kemampuan yang ditetapkan oleh COBIT.

Data sekunder diperoleh melalui studi literatur yang bertujuan untuk memperkuat landasan teoritis penelitian. Studi literatur mencakup teori dan konsep yang berkaitan dengan tata kelola teknologi informasi, keamanan data, manajemen risiko, serta framework COBIT 2019. Sumber literatur diperoleh dari buku referensi, jurnal ilmiah nasional dan internasional, e-book, standar resmi ISACA, ditambah rujukan dari berbagai studi terdahulu yang memiliki korelasi kuat dengan fokus bahasan ini.

2.3. Tinjauan Literatur

Peneliti menghimpun data sekunder melalui studi literatur untuk memperkokoh fondasi konseptual riset. Proses ini mencakup eksplorasi mendalam terhadap teori tata kelola TI, perlindungan informasi, serta manajemen risiko berbasis standar COBIT 2019. Referensi disintesis dari berbagai sumber otoritatif, mulai dari dokumen resmi ISACA dan buku referensi teknis, hingga publikasi ilmiah berskala nasional maupun internasional yang memiliki relevansi kuat dengan fokus bahasan ini.

2.4. Teknik Olah Data

Setelah seluruh data terhimpun, peneliti menerapkan analisis deskriptif-kualitatif untuk membedah fakta operasional di lapangan secara objektif. Proses evaluasi dilakukan dengan menyintesis temuan observasi, wawancara, dan kuesioner, lalu mengomparasikannya dengan standar COBIT 2019. Seluruh informasi ditelaah secara bertahap, mulai dari pemetaan kondisi eksisten hingga pengukuran level kapabilitas. Melalui pendekatan ini, identifikasi kesenjangan (*gap*) antara performa tata kelola saat ini dengan target ideal perusahaan dapat dirumuskan secara akurat.

2.5. Analisis Perhitungan dan Evaluasi

Analisis perhitungan dan evaluasi dilakukan berdasarkan hasil survei yang dikumpulkan dari responden PT Budi Gadai Indonesia. Tingkat kemampuan setiap proses COBIT dihitung dengan menjumlahkan skor untuk setiap item survei dan membagi totalnya dengan jumlah item untuk menghitung rata-rata.

Tingkat kemampuan yang dihitung digunakan sebagai indikator tingkat kemampuan setiap proses COBIT yang dianalisis dan berfungsi sebagai dasar untuk mengevaluasi pengaruh penerapan kerangka kerja COBIT 2019 terhadap peningkatan keamanan data dalam sistem informasi.

e-ISSN: 2798-9593
p-ISSN: 2798-9836

3. Hasil dam Pembahasan

PT Budi Gadai Indonesia adalah perusahaan gadai swasta di sektor jasa keuangan non-perbankan. Bisnis utamanya adalah menyediakan layanan pinjaman dengan jaminan barang berharga milik nasabah. Kantor-kantornya berlokasi strategis di daerah perkotaan, sehingga mudah diakses oleh nasabah dari berbagai latar belakang.

Sebagai perusahaan jasa keuangan, PT Budi Gadai Indonesia mengelola sejumlah besar data yang sangat rahasia, termasuk data pribadi nasabah, data transaksi keuangan, dan informasi tentang aset yang digadaikan. Karena alasan ini, sistem informasi merupakan elemen penting yang mendukung operasional bisnis perusahaan. Perusahaan terus mempromosikan penggunaan teknologi informasi untuk meningkatkan efisiensi operasional, memastikan transparansi, dan meningkatkan kepercayaan nasabah.

Namun, seiring dengan meluasnya penggunaan teknologi informasi, masalah yang berkaitan dengan keamanan data dan keandalan sistem juga meningkat. Oleh karena itu, implementasi Urgensi tata kelola TI yang efektif terletak pada perannya dalam memitigasi potensi ancaman, khususnya guna mencegah insiden kebocoran data serta degradasi performa sistem.

3.1. Infrastruktur TI dan SDM

Sinergi antara infrastruktur teknologi dan sumber daya manusia menjadi pilar utama dalam menunjang operasional bisnis PT Budi Gadai Indonesia. Komponen ini mencakup integrasi perangkat keras, piranti lunak, serta jaringan komunikasi yang difungsikan khusus untuk mengamankan data nasabah dan riwayat transaksi. Detail distribusi fasilitas teknologi pada berbagai unit kerja disajikan dalam tabel berikut:

Tabel 1
Fasilitas dan Sumber Daya Teknologi Informasi PT Budi Gadai Indonesia

No	Unit/Bagian	Fasilitas TI
1	Kantor Operasional	Komputer, Printer, Jaringan Internet
2	Bagian Administrasi	Sistem Informasi Nasabah, Database, Komputer
3	Bagian Keuangan	Sistem Transaksi Keuangan, Komputer, Printer
4	Bagian TI	Server, Perangkat Jaringan, Sistem Keamanan
5	Seluruh Unit	Akses Jaringan Internal dan Internet

Meskipun peralatan teknologi informasi ini memberikan kontribusi signifikan terhadap efisiensi bisnis, peralatan ini juga memerlukan manajemen dan langkah-langkah keamanan yang tepat.

3.2. Analisis Kematangan Keamanan Data

Studi ini menganalisis kematangan manajemen keamanan data untuk sistem informasi di PT Budi Gadai Indonesia berdasarkan kerangka kerja COBIT 2019. Analisis dilakukan dengan memilih domain dan proses COBIT 2019 yang terkait dengan keamanan data dan melakukan survei kuesioner kepada para pemangku kepentingan.

Tabel 2
Hasil Kuesioner Tingkat Kematangan Keamanan Data

Proses COBIT	Pertanyaan	Responden 1	Responden 2	Responden 3	Rata- rata
DSS05	Pengelolaan layanan keamanan data	4	4	5	4,33
DSS05	Pengendalian akses pengguna sistem	4	5	4	4,33
DSS06	Pengendalian proses bisnis berbasis TI	3	4	4	3,66
EDM03	Pengelolaan risiko keamanan data	4	4	3	3,66
EDM03	Monitoring dan evaluasi keamanan data	4	5	4	4,33

Rata-rata Tingkat Kematangan: 4,06

Hasil ini menunjukkan bahwa manajemen keamanan data PT Budi Gadai Indonesia secara umum berada pada tingkat yang baik, tetapi perlu optimasi lebih lanjut.

3.3. Evaluasi Kesenjangan Maturitas COBIT

Hasil kalkulasi tingkat kematangan digunakan untuk mengomparasikan performa aktual (*As-Is*) dengan ekspektasi masa depan (*To-Be*). Perbandingan mendalam ini disajikan pada tabel di bawah:

Tabel 3
Analisis Kematangan Proses COBIT

Kode	Deskripsi Proses	Aktual	Target
EDM01	*Governance Framework Setting*	4	5
EDM03	*Ensure Risk Optimization*	4	5
DSS05	*Manage Security Services*	4	5
DSS06	*Manage Business Process Controls*	4	5

Tingkat kematangan rata-rata secara keseluruhan adalah Level 4 (Terkelola dan Terukur), dengan target yang ditetapkan pada Level 5 (Dioptimalkan).

3.4. Identifikasi Disparitas

Hasil evaluasi menunjukkan adanya selisih (*gap*) sebesar satu tingkat antara pencapaian maturitas saat ini dengan target yang ditetapkan pada seluruh proses COBIT yang dianalisis.Kesenjangan ini menunjukkan bahwa meskipun PT Budi Gadai Indonesia telah menerapkan manajemen keamanan data yang sistematis dan terukur, peningkatan berkelanjutan, optimalisasi proses, dan peningkatan dokumentasi tetap menjadi area fokus. Hasil analisis ini akan menjadi dasar untuk merumuskan proposal perbaikan untuk meningkatkan keamanan data.

4. Penelitian

Berdasarkan pengamatan detail, tinjauan dokumen internal, dan wawancara terstruktur yang dilakukan padatahun 2020, manajemen keamanan data PT Budi Gadai Indonesia berada pada tahap yang sangat mendasar. Tata kelola TI pada saat itu tidak didasarkan pada kerangka kerja standar, dan langkah-langkah keamanan terutama bersifat reaktif daripada preventif.

Kerentanan yang sangat signifikan adalah manajemen akses pengguna secara manual. Karena penyediaan dan penghapusan akses merupakan proses manual, terdapat risiko tinggi "akun zombie" tetap aktif setelah karyawan keluar atau dipindahkan. Lebih lanjut, kurangnya standar enkripsi untuk data sensitif meningkatkan risiko kebocoran data, yang berpotensi mengakibatkan tanggung jawab hukum dan hilangnya kredibilitas perusahaan.

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Tabel 4

Hasil Pengukuran Tingkat Kemampuan Awal (Baseline 2020)

Kode Proses	Nama Proses COBIT	Skor Capaian	Kategori	Deskripsi Kondisi Eksisting
EDM03	Ensure Risk Optimization	2,1	Kurang	Manajemen risiko bersifat *ad-hoc*; belum ada *risk register* yang terdokumentasi secara formal.
DSS05	Manage Security	2,3	Kurang	Kontrol akses masih manual; enkripsi data belum diterapkan pada level database.
DSS06	Services	2,0	Kurang	Belum ada integrasi kontrol keamanan otomatis dalam alur transaksi harian.
APO13	Manage Business Process Controls	2,1	Kurang	Kebijakan keamanan informasi belum tersusun secara sistematis dan komprehensif.
Rata-rata	Manage Security	2,13	Kurang	Tata kelola berada pada level dasar (intuitif/tergantung individu).

4.1. Tahapan Adopsi Framework (2020–2025)

Transformasi tata kelola TI di PT Budi Gadai Indonesia dijalankan secara gradual selama periode lima tahun guna memfasilitasi adaptasi budaya organisasi. Strategi implementasi ini mengintegrasikan penguatan aspekteknis dengan pengembangan kapasitas SDM serta standarisasi prosedur yang menjadi fondasi utamakeamananinformasi perusahaan.

Tabel 5

Peta Jalan Strategis Implementasi COBIT

Tahun / Fase	Fokus Fokus Utama	Key Deliverables & Intervensi Teknologi
2020-2021 (Tahap I)	Tata Kelola & Risiko	Pembentukan struktur *IT Governance* dan penyusunan kebijakan keamanan sesuai standar COBIT.
2021-2023 (Tahap II)	Keamanan Operasional	Implementasi *Identity & Access Management* (IAM) dan enkripsi AES-256 pada seluruh data sensitif.
2023-2024 (Tahap III)	Kontrol Bisnis Terpadu	Digitalisasi kontrol internal pada aplikasi inti operasional untuk mencegah *fraud* sistemik.
2024-2025 (Tahap IV)	Resiliensi & Optimasi	Pemasangan SIEM untuk deteksi ancaman *real-time* dan program *Security Awareness* massal.

4.2. Analisis Hasil Implementasi dan Dampak Strategis

Melalui intervensi sistematis selama lima tahun, postur keamanan perusahaan telah ditingkatkan secara fundamental. Adopsi manajemen identitas dan akses (IAM) sejak tahun 2022 telah menghilangkan kesalahan manusia dalam manajemen akun dan mencapai kontrol akses yang ketat berdasarkan prinsip hak akses minimal.

Dalam hal perlindungan data, penerapan AES-256 (Advanced Encryption Standard) menciptakan lapisan perlindungan ganda untuk data yang tersimpan dan data yang sedang ditransmisikan. Selain itu, pengenalan sistem SIEM (Security Information and Event Management) pada tahun 2023 memberikan visibilitas langsung terhadap anomali jaringan, secara dramatis mengurangi waktu respons terhadap upaya serangan siber.

4.3. Pengukuran Efektivitas Implementasi dan Verifikasi Empiris

Efektivitas implementasi kerangka kerja COBIT diukur dengan membandingkan indikator kinerja utama (KPI) antara tahun 2020 dan 2025. Data tersebut menegaskan bahwa pendekatan sistematis berdasarkan kerangka kerja internasional secara signifikan mengurangi risiko keamanan.

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Tabel 6

Perbandingan KPI Keamanan Informasi

Parameter Efektivitas	Baseline (2020)	Capaian (2025)	Efisiensi / Peningkatan
Insiden Keamanan (Rata-rata per Bulan)	12,0 Insiden	3,8 Insiden	Penurunan 68,3%
Waktu Respon Insiden (Mean Time to Respond)	8,5 Jam	2,3 Jam	Penurunan 72,9%
Kesadaran Keamanan Karyawan (User Awareness)	45,0%	82,0%	Peningkatan 37,0%
Kepatuhan Kebijakan (Compliance Rate)	52,0%	89,0%	Peningkatan 37,0%

Peningkatan kapabilitas ini divalidasi dengan skor akhir yang menunjukkan bahwa perusahaan kini berada pada level yang jauh lebih stabil dan terukur.

Tabel 7

Perbandingan Skor Kemampuan Proses COBIT

Kode Proses	Fokus Area Penilaian	Skor 2020	Skor 2025	Persentase Peningkatan
EDM03	Ensure Risk Optimization	2,1	4,2	100,0%
DSS05	Manage Security Services	2,3	4,4	91,3%
DSS06	Manage Business Process Controls	2,0	4,1	105,0%
APO13	Manage Security	2,1	4,3	104,8%
DSS02	Manage Service Requests & Incidents	2,6	4,2	61,5%
Rata-rata	Indeks Kapabilitas Kumulatif	2,22	4,24	91,0%

Secara keseluruhan, temuan empiris dalam penelitian ini menegaskan bahwa implementasi framework COBIT pada PT Budi Gadai Indonesia tidak hanya meningkatkan aspek teknis keamanan data, tetapi juga menciptakan ekosistem tata kelola TI yang logis, akuntabel, dan adaptif terhadap dinamika ancaman siber di masa depan.

5. Penutup

Evaluasi mendalam terhadap penerapan kerangka kerja COBIT di PT Budi Gadai Indonesia selama periode 2020–2025 memberikan gambaran signifikan mengenai transformasi tata kelola perusahaan. Hasil penelitian menunjukkan bahwa implementasi COBIT berhasil mengubah tingkat tata kelola keamanan data secara dramatis, di mana skor kemampuan rata-rata melonjak dari 2,22 pada kategori rendah menjadi 4,24 pada kategori baik di tahun 2025. Pencapaian ini membuktikan keberhasilan transisi perusahaan dari manajemen TI yang bersifat intuitif dan ad-hoc menuju tata kelola yang terukur, terstandarisasi, serta teroptimalkan. Efektivitas tersebut juga didukung oleh adopsi manajemen identitas dan akses (IAM) serta teknologi enkripsi AES-256 yang secara nyata memitigasi risiko teknis dan mengurangi celah keamanan kritis. Hal ini dibuktikan dengan penurunan frekuensi insiden keamanan sebesar 68,3% serta percepatan waktu respons insiden (MTTR) mencapai 72,9%, yang memperkuat ketahanan sistem informasi secara menyeluruh. Lebih lanjut, penerapan domain DSS06 telah berhasil mensinkronisasikan aspek keamanan ke dalam setiap alur kerja operasional melampaui batasan departemen TI, yang tercermin pada kenaikan kesadaran keamanan personel dari 45% menjadi 82%. Secara kolektif, hasil ini mengindikasikan telah terbentuknya budaya sadar risiko yang merata di seluruh level organisasi PT Budi Gadai Indonesia.

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Tabel 8

Ringkasan Pencapaian Strategis (2020 vs. 2025)

Dimensi Penilaian	Kondisi Baseline (2020)	Kondisi Final (2025)	Dampak Strategis
Tingkat Kapabilitas	2,22 (Level 2)	4,24 (Level 4)	Tata kelola terukur secara kuantitatif.
Manajemen Akses	Manual / Berisiko	Otomatis (IAM)	Eliminasi akun tidak sah & human error.
Proteksi Data	Tanpa Enkripsi	Enkripsi AES-256	Jaminan kerahasiaan data nasabah.
Monitoring	Reaktif	Proaktif (SIEM)	Deteksi ancaman secara real-time.
Budaya Organisasi	Rendah (45%)	Tinggi (82%)	Keamanan menjadi tanggung jawab bersama.

Audit Independen Berkelanjutan: Kami merekomendasikan agar pakar eksternal melakukan audit keamanan informasi setidaknya setiap tahun untuk memastikan bahwa standar COBIT diimplementasikan secara objektif dan konsisten.

Berkembang ke COBIT 2019 Terbaru: Mengingat pesatnya inovasi teknologi, perusahaan harus mempertimbangkan untuk mengadopsi panduan desain COBIT 2019 terbaru, yang mencakup "area fokus" seperti keamanan cloud dan tata kelola AI, seiring dengan perluasan transformasi digital mereka.

Memperbarui Rencana Pemulihan Bencana (DRP): Meskipun skor DSS05 bagus, untuk melawan ancaman siber yang semakin canggih seperti ransomware, simulasi pemulihan bencana secara berkala harus terus dilakukan untuk menjaga agar rencana tetap mutakhir.

Ucapan Terima Kasih

Sebagai penutup, penulis ingin mengungkapkan rasa terima kasih yang mendalam kepada semua pihak yang telah memfasilitasi penelitian ini. Keberhasilan transformasi tata kelola keamanan informasi ini merupakan hasil kerja.

Daftar Pustaka

[1] Susanto, A., & Meiryani. (2021). Tata kelola teknologi informasi dan perannya dalam peningkatan kinerja organisasi. Jurnal Sistem Informasi, 17(2), 85–96.
[2] Putra, R. A., & Pratama, D. (2022). Analisis risiko keamanan data pada perusahaan jasa keuangan non-bank. Jurnal Keamanan Informasi dan Teknologi, 6(1), 23–34.
[3] Rahmawati, N., & Hidayat, T. (2021). Dampak kelemahan pengendalian TI terhadap keamanan data dan kepercayaan pengguna. Jurnal Informatika dan Manajemen, 9(3), 112–121.
[4] M. A. Andyas, et al., "Manajemen keamanan informasi transformasi digital insurco berbasis COBIT 2019," Zonasi, vol. 5, no. 3, pp. 452–467, 2023.Sari, D. P., & Nugroho, E. (2022). Evaluasi tata kelola keamanan informasi menggunakan framework COBIT 2019. Jurnal Teknologi Informasi dan Audit Sistem, 4(2), 55–66.
[5] R. Ramdani, et al., "Ambidextrous AI Governance Model for Bank Digital Transformation," Jurnal Jutif, 2023. [Online]. Available: https://jutif.if.unsoed.ac.id/M. A. Andyas, R. Mulyana, and W. A. Nurtrisha, “Manajemen keamanan informasi untuk transformasi digital insurco berbasis cobit 2019 focus area information security,” Zonasi, vol. 5, no. 3, pp. 452–467, Oct. 2023, doi: 10.31849/zn.v5i3.15275.
[6] G. Falzone, "IT Governance Maturity Assessment for Italian Banking," Politecnico di Torino, 2023. [Online]. Available: https://webthesis.biblio.polito.it/G. Falzone, “IT Governance Maturity Assessment: rilevazione del livello di maturità dei processi IT per una Banca italiana= IT Governance Maturity Assessment: assessing the level …”, [Online]. Available: https://webthesis.biblio.polito.it/34187/
[7] F. Adrian & G. Wang, "Capability Level of IT Governance for Cybersecurity in Banking," JATIT, vol. 101, no. 5, 2023. [Online]. Available: http://www.jatit.org/ Daerah Papua,” International Journal of Engineering, Science and Information Technology, vol. 4, no. 4, Nov. 2024, doi: 10.52088/ijesty.v4i4.609.
[8] Lompoliu & G. Tangka, "IT Governance using COBIT 2019 at Bank Papua," IJESTY, vol. 4, no. 4, 2024. doi: 10.52088/ijesty.v4i4.609.N. Rashikha, R. Mulyana, and R. Hanafi, “Using COBIT 2019 SME for Digital Transformation Governance of BPRDCo,” Jutisi : Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, Dec. 2024, doi: 10.35889/jutisi.v13i3.2250.
[9] S. Sherly & M. I. Fianty, "Fintech Operations Evaluation via COBIT 2019 Framework," Jurnal Riset Informatika, 2024. doi: 10.34288/jri.v6i2.267.P. Widharto, Z. Suhatman, and R. F. Aji, “Measurement of information technology governance capability level: a case study of PT Bank BBS,” TELKOMNIKA Telecommunication Computing Electronics and Control, vol. 20, no. 2, pp. 296–296, Apr. 2022, doi: 10.12928/telkomnika.v20i2.21668.
[10] N. Rashikha, et al., "COBIT 2019 SME for Digital Transformation Governance," Jutisi, vol. 13, no. 3, 2024. doi: 10.35889/jutisi.v13i3.2250.

[11] A. Asmah & M. Kyobe, "Impact of Audit on IT Governance in Ghana Financial Sector," Wiley Online Library, 2024. doi: 10.1002/isd2.12349.
[12] P. Widharto, et al., "IT Governance Capability Level Measurement: PT Bank BBS Case Study," TELKOMNIKA, vol. 20, no. 2, pp. 296, 2022. doi: 10.12928/telkomnika.v20i2.21668.
[13] N. Susanto & A. Meiryani, "Peran tata kelola TI dalam peningkatan kinerja organisasi," Jurnal Sistem Informasi, vol. 13, no. 2, 2021.