Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id

E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep

OPEN ACCESS

https://doi.org/10.35870/siskom.v6i3.1973

Evaluasi Tata Kelola Teknologi Informasi pada Bank PT BPR NTB Persero dengan Menggunakan COBIT 5 dan ISO/IEC 27001

Gina Mahligai Putri [1*], Khairan Marzuki [2], Andi Sofyan Anas [3], Ondi Asroni [4], Wisnu Alfiansyah [5]

[1*,2,3,4,5] Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Bumigora, Kota Mataram, Nusa Tenggara Barat, Indonesia.

Corresponding Email: mahligaiputrigina@gmail.com [1*]

Histori Artikel:
Dikirim 14 Jul 2026; *Diterima dalam bentuk revisi* 02 Agus 2026; *Diterima* 13 Agus 2026; *Diterbitkan* 28 Agus 2026.

Abstrak

Perkembangan Teknologi Informasi (TI) mendorong penggunaan core banking system berbasis cloud sebagai infrastruktur utama dalam operasional perbankan. Ketergantungan PT Bank BPR NTB Perseroda terhadap sistem ini memerlukan tata kelola TI yang menjamin ketersediaan layanan, keandalan sistem, dan keamanan informasi. Hasil observasi dan wawancara menunjukkan adanya gangguan jaringan layanan cloud, pasokan listrik, serta potensi ancaman keamanan siber yang berdampak pada keterlambatan proses kredit dan transaksi nasabah. Penelitian ini bertujuan mengevaluasi efektivitas tata kelola TI menggunakan COBIT 5 dan mengidentifikasi implementasi kontrol keamanan informasi berdasarkan ISO/IEC 27001:2022. Domain COBIT 5 yang digunakan meliputi EDM01, APO12, DSS01, dan MEA03, sedangkan kontrol ISO/IEC 27001:2022 mencakup A.5.1, A.5.23, dan A.5.30. Metode yang diterapkan adalah mixed methods melalui wawancara, observasi, studi dokumentasi, dan kuesioner terhadap 32 responden. Analisis data dilakukan dengan Process Assessment Model (PAM) COBIT 5. Hasil penelitian menunjukkan nilai kapabilitas rata-rata sebesar 3,30 hingga 3,38, yang menunjukkan bahwa proses tata kelola telah diterapkan, tetapi pengelolaan risiko dan pemantauan operasional masih perlu ditingkatkan. Penelitian ini menyimpulkan bahwa integrasi COBIT 5 dan ISO/IEC 27001:2022 memberikan evaluasi komprehensif terhadap tata kelola dan keamanan informasi.

Kata Kunci: Capability Level; COBIT 5; Core Banking System; ISO/IEC 27001:2022; Keamanan Informasi; Tata Kelola Teknologi Informasi.

Abstract

The advancement of Information Technology (IT) has driven the use of cloud-based core banking systems as the primary infrastructure in banking operations. PT Bank BPR NTB Perseroda's reliance on this system necessitates IT governance that ensures service availability, system reliability, and information security. Observations and interviews reveal issues such as cloud service network disruptions, power supply interruptions, and potential cybersecurity threats impacting the timeliness of credit processes and customer transactions. This study aims to evaluate the effectiveness of IT governance using COBIT 5 and identify the implementation of information security controls based on ISO/IEC 27001:2022. The COBIT 5 domains utilized include EDM01, APO12, DSS01, and MEA03, while the ISO/IEC 27001:2022 controls encompass A.5.1, A.5.23, and A.5.30. A mixed methods approach was employed through interviews, observations, document studies, and questionnaires involving 32 respondents. Data analysis was conducted using the Process Assessment Model (PAM) of COBIT 5. The results indicate average capability levels ranging from 3.30 to 3.38, suggesting that governance processes have been implemented but that risk management and operational monitoring require enhancement. This study concludes that the integration of COBIT 5 and ISO/IEC 27001:2022 provides a comprehensive evaluation of governance and information security.

Keyword: Capability Level; COBIT 5; Core Banking System; ISO/IEC 27001:2022; Information Security; IT Governance.

Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id
E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

1. Pendahuluan

Menurut (Hidayah *et al.,* 2024) Perkembangan teknologi informasi telah memberikan kontribusi yang besar terhadap transformasi industri perbankan melalui peningkatan efisiensi operasional, percepatan layanan, serta pengelolaan data dan informasi yang lebih akurat. Salah satu implementasi teknologi informasi yang menjadi pendukung utama operasional perbankan adalah Core Banking System (CBS), yang digunakan untuk mengelola transaksi simpanan, layanan kredit, serta penyediaan laporan yang mendukung kebutuhan manajemen dan pemenuhan regulasi (Hanif *et al.,* 2025).

Meningkatnya ketergantungan organisasi terhadap Core Banking System menjadikan tata kelola teknologi informasi (IT Governance) sebagai faktor penting dalam mendukung keberhasilan operasional perbankan. Tata kelola teknologi informasi berperan dalam memastikan bahwa pemanfaatan teknologi informasi mampu mendukung pencapaian tujuan organisasi, mengoptimalkan pemanfaatan sumber daya, mengelola risiko teknologi informasi, serta memenuhi ketentuan regulasi yang berlaku. Dengan semakin kompleksnya kebutuhan bisnis dan tingginya ketergantungan terhadap sistem informasi, organisasi memerlukan mekanisme tata kelola yang sistematis dan terukur agar layanan teknologi informasi dapat berjalan secara efektif, efisien, dan berkelanjutan (Yuanita *et al.,* 2025).

Keamanan informasi merupakan elemen yang memiliki peran penting dalam mendukung operasional Core Banking System, khususnya pada lingkungan komputasi berbasis cloud (Tanjung *et al.,* 2025). Core Banking System berfungsi mengelola berbagai informasi penting, seperti data nasabah, transaksi keuangan, serta aset informasi lainnya yang harus dijamin kerahasiaan (confidentiality), integritas (integrity), dan ketersediaannya (availability) (Prasetya *et al.,* 2025). Penerapan kontrol keamanan informasi menjadi faktor yang sangat penting untuk mendukung efektivitas tata kelola teknologi informasi sekaligus memastikan keberlangsungan operasional layanan perbankan (Lestari *et al.,* 2025).

PT BPR NTB Perseroda merupakan Bank Perekonomian Rakyat salah satu Perusahaan Milik Pemerintah Daerah yang bergerak dalam bidang Jasa Keuangan/Perbankan yang berlokasi di Wilayah Mataram yang telah memanfaatkan Core Banking System berbasis Cloud sebagai sistem utama dalam mendukung operasional perbankan. Sistem ini digunakan untuk mengelola penghimpunan dana, penyaluran kredit, transaksi keuangan, serta layanan digital kepada nasabah (Gade., 2025).

Berdasarkan hasil observasi dan wawancara yang dilakukan dengan Sub Divisi Operasional Teknologi dan Informasi PT Bank BPR NTB Perseroda, operasional Core Banking System masih menghadapi beberapa kendala, seperti gangguan pada jaringan layanan cloud, ketidakstabilan pasokan listrik, serta potensi ancaman keamanan siber. Kondisi tersebut berdampak pada terhambatnya proses kredit, terganggunya transaksi nasabah secara real-time, dan menurunnya efektivitas pelayanan operasional (Hanif *et al.,* 2025). Meskipun setiap gangguan telah ditangani sesuai dengan prosedur operasional yang berlaku, hingga saat ini belum pernah dilakukan evaluasi secara komprehensif terhadap efektivitas tata kelola teknologi informasi, khususnya dalam mengelola risiko, menjamin keberlangsungan operasional, dan mendukung penerapan keamanan informasi pada Core Banking System. Oleh karena itu, fokus utama penelitian ini bukan pada keberadaan gangguan operasional itu sendiri, melainkan pada belum adanya informasi yang menggambarkan sejauh mana tata kelola teknologi informasi telah diterapkan secara efektif untuk mendukung keandalan, keamanan, dan keberlangsungan layanan Core Banking System (M. Radhiya Amiryan Ahadis, *et al.,* 2025).

Beberapa penelitian terdahulu telah mengevaluasi tata kelola teknologi informasi dan keamanan informasi menggunakan framework COBIT maupun kombinasi COBIT dengan ISO/IEC 27001.

Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id
E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

Tabel 1. Penelitian Terdahulu

Penulis	Framework	Temuan	Keterbatasan (Research Gap)
(Hanif *et al.*, 2025)	COBIT & ISO/IEC 27001	Integrasi COBIT dan ISO meningkatkan efektivitas audit TI, manajemen risiko, dan keselarasan TI.	Bersifat *literature review* dan belum diterapkan pada operasional *core banking system* berbasis *cloud*.
(Yoga *et al.*, 2024)	COBIT 5 & ISO/IEC 27001:2013	Audit keamanan informasi menghasilkan Capability Level 1 dengan target Level 3.	Menggunakan ISO/IEC 27001:2013 dan objek penelitian non-perbankan.
(Nawir *et al.*, 2022)	COBIT 2019 & ISO/IEC 27001:2013	Menghasilkan rekomendasi peningkatan keamanan informasi pada aplikasi *smart tourism*.	Menggunakan COBIT 2019 dan ISO/IEC 27001:2013 serta tidak diterapkan pada sektor perbankan.
(Yuanita Pratiwi & Linda Wahyu Widianti, 2025)	COBIT 5	Tingkat kapabilitas tata kelola TI berada pada Level 4.	Hanya menggunakan COBIT 5 tanpa mengintegrasikan standar keamanan informasi.
(Daffa Iqbal Agselmora & Utomo, 2022)	COBIT 5 (DSS)	Audit tata kelola TI menghasilkan Maturity Level 3,89 dan Capability Level 2.	Hanya menggunakan COBIT 5 dan diterapkan pada lingkungan perguruan tinggi.

Meskipun berbagai penelitian telah memberikan kontribusi dalam bidang tata kelola teknologi informasi dan keamanan informasi, masih terdapat sejumlah keterbatasan. Sebagian besar penelitian hanya mengkaji domain tertentu, masih mengacu pada standar ISO/IEC 27001:2013, atau dilakukan pada organisasi di luar sektor perbankan. Di samping itu, penelitian yang secara khusus mengombinasikan evaluasi tata kelola teknologi informasi dan implementasi kontrol keamanan informasi pada Core Banking System berbasis cloud di lingkungan Bank Perekonomian Rakyat masih relatif sedikit. Oleh karena itu, penelitian ini bertujuan untuk mengisi kesenjangan tersebut melalui penerapan framework COBIT 5 yang dipadukan dengan standar ISO/IEC 27001:2022 pada PT Bank BPR NTB Perseroda.

Penelitian ini menggunakan framework COBIT 5 karena mampu mengevaluasi efektivitas tata kelola teknologi informasi melalui pengukuran tingkat kapabilitas proses. COBIT 5 menyediakan mekanisme evaluasi yang mencakup aspek tata kelola, manajemen risiko, operasional, dan kepatuhan terhadap regulasi (Kristen & Wacana, 2025). Sementara itu, ISO/IEC 27001:2022 digunakan sebagai standar acuan dalam mengidentifikasi implementasi kontrol keamanan informasi yang mendukung kerahasiaan, integritas, dan ketersediaan informasi (Frangky & Sinaga, 2024). Dengan demikian, COBIT 5 dan ISO/IEC 27001:2022 memiliki fungsi yang saling melengkapi, yaitu COBIT 5 mengevaluasi efektivitas tata kelola teknologi informasi, sedangkan ISO/IEC 27001:2022 digunakan untuk mengidentifikasi penerapan kontrol keamanan informasi.

Domain EDM01 dipilih untuk mengevaluasi efektivitas kerangka tata kelola serta mekanisme pengawasan teknologi informasi dalam organisasi. APO12 digunakan karena penelitian ini berfokus pada pengelolaan risiko yang berkaitan dengan gangguan jaringan layanan cloud, ketidakstabilan pasokan listrik, dan potensi ancaman keamanan siber yang dapat memengaruhi operasional Core Banking System. Selanjutnya, DSS01 diterapkan untuk menilai efektivitas pengelolaan operasional Core Banking System, yang mencakup kegiatan pemantauan layanan, penanganan gangguan, serta pengelolaan lingkungan operasional. Adapun MEA03 digunakan untuk mengevaluasi tingkat kepatuhan terhadap regulasi yang berlaku sekaligus menilai tindak lanjut hasil evaluasi sebagai upaya peningkatan tata kelola teknologi informasi. Keempat domain tersebut dipilih karena dinilai paling sesuai dengan karakteristik permasalahan yang teridentifikasi pada operasional Core Banking System di PT Bank BPR NTB Perseroda (ISACA, 2012).

Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id
E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

Berdasarkan permasalahan yang telah diidentifikasi, penelitian ini menggunakan framework COBIT 5 yang didukung oleh ISO/IEC 27001:2022 untuk mengevaluasi tata kelola teknologi informasi dan implementasi kontrol keamanan informasi pada operasional Core Banking System berbasis cloud. Melalui evaluasi tersebut, penelitian ini bertujuan mengidentifikasi kesenjangan antara kondisi saat ini dengan kondisi yang diharapkan serta menghasilkan rekomendasi perbaikan guna meningkatkan efektivitas tata kelola teknologi informasi di PT BPR NTB Perseroda.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan deskriptif-evaluatif dengan metode campuran (mixed methods), yaitu mengombinasikan pendekatan kualitatif dan kuantitatif (Pratiwi *et al.,* 2025). Pendekatan kualitatif dilakukan melalui wawancara, observasi, dan studi dokumentasi (Negeri *et al.,* 2024). Sementara itu, pendekatan kuantitatif digunakan untuk mengukur tingkat kapabilitas tata kelola teknologi informasi menggunakan framework COBIT 5. Pengumpulan data dilakukan melalui wawancara, observasi, studi dokumentasi, dan kuesioner. Responden penelitian berjumlah 32 orang. Pemilihan domain dilakukan berdasarkan kesesuaian dengan permasalahan penelitian. EDM01 digunakan untuk mengevaluasi mekanisme tata kelola dan pengawasan teknologi informasi, APO12 untuk mengevaluasi pengelolaan risiko yang berkaitan dengan gangguan jaringan *cloud*, pasokan listrik, dan ancaman keamanan siber, DSS01 untuk mengevaluasi efektivitas operasional *Core Banking System*, sedangkan MEA03 digunakan untuk mengevaluasi kepatuhan terhadap regulasi serta tindak lanjut hasil evaluasi yang dilakukan organisasi.

Analisis data pada penelitian ini dilakukan menggunakan Process Assessment Model (PAM) COBIT 5. Model tersebut digunakan sebagai pedoman untuk mengukur tingkat kapabilitas (capability level) pada setiap domain. Selanjutnya, hasil pengukuran dibandingkan antara kondisi aktual (as-is) dan kondisi yang diharapkan (to-be) melalui analisis kesenjangan (gap analysis), yang kemudian dijadikan dasar dalam penyusunan rekomendasi perbaikan guna meningkatkan efektivitas tata kelola teknologi informasi (ISACA, 2012).

Dalam penelitian ini, ISO/IEC 27001:2022 tidak digunakan sebagai dasar audit sertifikasi maupun untuk mengukur tingkat kepatuhan organisasi, tetapi sebagai acuan dalam mengidentifikasi implementasi kontrol keamanan informasi yang mendukung operasional Core Banking System. Kontrol yang dianalisis meliputi A.5.1 (Information Security Policies), A.5.23 (Information Security for Use of Cloud Services), dan A.5.30 (ICT Readiness for Business Continuity). Hasil wawancara dan observasi selanjutnya dianalisis secara deskriptif untuk menggambarkan penerapan kontrol tersebut serta melengkapi hasil evaluasi tata kelola teknologi informasi menggunakan COBIT 5.

3. Hasil dan Pembahasan

3.1. Hasil

3.1.1 Initiation

Pada tahap ini, peneliti menetapkan ruang lingkup penelitian dengan menentukan objek penelitian, yaitu operasional core banking system pada PT BPR NTB Perseroda. Selanjutnya dilakukan pengumpulan data awal berupa profil organisasi, visi dan misi, struktur organisasi, tugas dan fungsi Divisi Operasional Teknologi dan Informasi, serta dokumen yang berkaitan dengan pengelolaan teknologi informasi. Peneliti juga melakukan wawancara awal dengan Pemimpin Sub Divisi Operasional Teknologi dan Informasi untuk memperoleh gambaran mengenai kondisi tata kelola TI, operasional core banking system, serta permasalahan yang dihadapi dalam mendukung layanan perbankan. Berdasarkan data yang diperoleh, peneliti mengidentifikasi Enterprise Goals, IT-related Goals, serta permasalahan utama, seperti downtime, gangguan layanan cloud, dan risiko keamanan informasi.

Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id
E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

3.1.2 Planning and Assessment

Pada tahap Planning, peneliti menyusun rencana penelitian dengan menetapkan responden, metode pengumpulan data, serta instrumen yang akan digunakan dalam proses evaluasi. Pemilihan responden dilakukan menggunakan teknik purposive sampling, yaitu berdasarkan kriteria dan peran yang telah ditentukan melalui RACI Chart. Responden dalam penelitian ini terdiri atas Pemimpin Sub Divisi TI, Bagian Kepatuhan, Pemimpin Sub Divisi Kredit, Bagian Analisis Kredit, serta perwakilan kantor cabang yang terlibat dalam operasional core banking system.

3.1.3 Briefing

Tahap briefing memastikan pemahaman yang seragam mengenai tujuan dan proses audit kepada seluruh narasumber Sebelum proses pengumpulan data dilaksanakan (Ramadhian *et al.,* 2025). Peneliti memberikan penjelasan kepada responden mengenai tujuan penelitian, manfaat penelitian, serta tata cara pengisian kuesioner menggunakan skala Likert 1–5 agar setiap Pernyataan dapat dipahami dengan baik.

3.1.4 Data Collection

Pada tahap Data Collection, peneliti melakukan pengumpulan data yang diperlukan untuk mengevaluasi tata kelola teknologi informasi pada operasional core banking system PT BPR NTB Perseroda.

Tabel 2. Hasil Temuan Wawancara

Sub Domain	Temuan Wawancara
EDM01	PT BPR NTB Perseroda telah memiliki kebijakan dan SOP TI yang mengacu pada regulasi OJK. Tata kelola TI diterapkan melalui monitoring operasional, pelaporan berkala, serta prosedur pengembangan dan perubahan sistem yang terdokumentasi.
APO12	Manajemen risiko TI dilakukan melalui identifikasi, monitoring, dan dokumentasi risiko. Risiko utama meliputi *downtime*, gangguan jaringan dan layanan *cloud*, *human error*, serta kepatuhan terhadap regulasi.
DSS01	Operasional *core banking system* telah didukung SOP, monitoring harian, penanganan insiden, mekanisme *backup* dan *failover*, serta *Data Recovery Center (DRC)* untuk menjaga keberlangsungan layanan.
MEA03	Kepatuhan terhadap regulasi dipantau melalui audit internal dan eksternal, monitoring operasional, serta tindak lanjut atas setiap temuan audit sebagai upaya peningkatan layanan TI.

3.1.5 Data Validation

Uji validitas dilakukan untuk memastikan bahwa setiap item pernyataan dalam kuesioner mampu mengukur variabel yang diteliti secara tepat. Pengujian validitas menggunakan metode Pearson Product Moment dengan membandingkan nilai koefisien korelasi (r hitung) terhadap nilai r tabel pada tingkat signifikansi yang telah ditentukan (Zayrin *et al.,* 2025). Hasil pengujian menunjukkan bahwa seluruh item pernyataan memiliki nilai r hitung yang lebih besar daripada r-tabel, sehingga seluruh item dinyatakan valid dan layak digunakan dalam proses pengumpulan data.

Tabel 3. Hasil Uji Validitas Kuesioner

Aspek Fokus	Indikator	R hitung	R tabel	Kesimpulan
EDM01.01	P1	0.586	0.349	Valid
	P2	0.515	0.349	Valid
EDM01.02	P3	0.537	0.349	Valid
	P4	0.662	0.349	Valid

Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id
E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

APO12.01	P5	0.530	0.349	Valid
	P6	0.520	0.349	Valid
APO12.02	P7	0.547	0.349	Valid
	P8	0.573	0.349	Valid
APO12.06	P9	0.565	0.349	Valid
	P10	0.520	0.349	Valid
	P11	0.528	0.349	Valid
DSS01.01	P12	0.498	0.349	Valid
	P13	0.674	0.349	Valid
DSS01.03	P14	0.542	0.349	Valid
	P15	0.509	0.349	Valid
DSS01.04	P16	0.517	0.349	Valid
	P17	0.547	0.349	Valid
MEA03.01	P18	0.679	0.349	Valid
	P19	0.720	0.349	Valid
MEA03.02	P20	0.535	0.349	Valid

Selanjutnya uji reliabilitas dilakukan untuk mengukur tingkat konsistensi instrumen penelitian dalam mengumpulkan data. Pengujian reliabilitas menggunakan metode Cronbach's Alpha, di mana suatu instrumen dinyatakan reliabel apabila memiliki nilai Cronbach's Alpha lebih besar dari 0,60. Hasil pengujian menunjukkan bahwa nilai Cronbach's Alpha instrumen penelitian berada di atas batas minimum yang ditetapkan, sehingga seluruh item pernyataan dinyatakan reliabel (Forester *et al.,* 2024).

Tabel 4. Hasil Uji Reliabilitas Kuesioner

Sub Domain	Cronbach's Alpha	Keterangan
EDM01	0.624	Reliabel
APO12	0.674	Reliabel
DSS01	0.686	Reliabel
MEA03	0.729	Reliabel

3.1.6 Process Atribute Level

Peneliti melakukan penentuan tingkat kapabilitas (capability level) dari setiap sub proses yang dievaluasi berdasarkan data kuesioner yang telah direkapitulasi. Penentuan tingkat kapabilitas dilakukan melalui perhitungan Nilai Kapabilitas (NK) yang selanjutnya dikonversikan ke dalam Level 0–5 sesuai dengan Process Assessment Model (PAM) COBIT 5. Target kondisi yang diharapkan (to-be) ditetapkan pada Level 4 (Predictable Process) berdasarkan hasil wawancara dengan Pemimpin Sub Divisi Informasi dan Teknologi.

Tabel 5. Penentuan Gap Sub Proses keseluruhan COBIT 5

Domain	Proses	As-is	To-be	Gap
EDM01.01	*Evaluate the governance system*	3.20	4	0.80
EDM01.03	*Monitor the governance system*	3.39	4	0.61
APO12.01	*Collect data*	3.37	4	0.63
APO12.02	*Analyse risk*	3.29	4	0.71
APO12.06	*Respond to risk*	3.29	4	0.71
DSS01.01	*Perform operational procedures*	3.23	4	0.77
DSS01.03	*Monitor IT infrastructure*	3.18	4	0.82
DSS01.04	*Manage the environment*	3.32	4	0.68
MEA03.01	*Identify external compliance requirements*	3.42	4	0.58
MEA03.03	*Confirm external compliance*	3.34	4	0.66

Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id
E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

Rata-rata	3.30	4	0.70

Berdasarkan Tabel 4, seluruh subproses yang dievaluasi berada pada Capability Level 3 (Established Process) dengan rata-rata nilai kapabilitas sebesar 3,30 dan gap sebesar 0,70 terhadap target Level 4 (Predictable Process). Hasil ini menunjukkan bahwa proses tata kelola teknologi informasi di PT BPR NTB Perseroda telah terdokumentasi dan diterapkan secara konsisten, namun belum sepenuhnya didukung oleh mekanisme pengukuran, pemantauan, dan pengendalian yang terukur. Kondisi tersebut berpotensi memengaruhi efektivitas operasional core banking system, terutama pada proses monitoring infrastruktur, pengelolaan risiko, dan penanganan gangguan yang dapat berdampak pada kontinuitas layanan. Oleh karena itu, prioritas perbaikan perlu difokuskan pada domain DSS01 dan APO12 yang memiliki nilai gap terbesar, sedangkan EDM01 dan MEA03 diarahkan pada penguatan evaluasi tata kelola serta tindak lanjut kepatuhan agar target Capability Level 4 (Predictable Process) dapat dicapai.

Tabel 6. Dampak Terhadap CBS

Domain/Proses	Gap	Dampak terhadap Core Banking System	Prioritas
EDM01	0.61–0.80	Evaluasi tata kelola dan kebijakan masih perlu ditingkatkan agar pengawasan lebih konsisten.	Sedang
APO12	0.63–0.71	Risiko operasional belum sepenuhnya mampu diantisipasi sehingga berpotensi menyebabkan gangguan layanan.	Tinggi
DSS01	0.68–0.82	Monitoring infrastruktur yang belum optimal berpotensi meningkatkan downtime dan mengganggu operasional Core Banking System.	Sangat Tinggi
MEA03	0.58–0.66	Kepatuhan telah berjalan baik, namun tindak lanjut hasil audit masih perlu diperkuat.	Rendah–Sedang

3.1.7 Reporting The Result

Tabel 6. Gap dan Rekomendasi

Domain	Temuan	Gap	Rekomendasi
EDM01.01 (Evaluate The Governance System)	BPR telah memiliki kebijakan dan SOP tata kelola TI yang mengacu pada regulasi OJK. Proses pengelolaan dan perubahan *core banking system* telah dilaksanakan secara terdokumentasi.	Penerapan tata kelola TI belum sepenuhnya terukur, dievaluasi secara berkala, dan konsisten di seluruh unit kerja.	Melakukan evaluasi berkala terhadap implementasi kebijakan dan SOP, menetapkan KPI tata kelola TI
EDM01.03 (Monitor the governance system)	BPR telah menerapkan monitoring tata kelola TI melalui laporan berkala, monitoring operasional harian, serta pelaporan gangguan.	Hasil monitoring belum dimanfaatkan secara optimal untuk perbaikan berkelanjutan.	Meningkatkan evaluasi berkala dan digitalisasi monitoring.
APO12.01 (Collect data)	BPR telah melakukan pengumpulan dan pendokumentasian data risiko TI melalui monitoring harian, pencatatan insiden, dan profil risiko.	Data risiko belum dimanfaatkan secara optimal sebagai dasar evaluasi.	Mengembangkan Risk Register TI terintegrasi untuk mendokumentasikan risiko, penyebab, dampak, penanganan, dan status penyelesaiannya

Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id
E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

APO12.02 (Analyse risk)	BPR telah melakukan analisis risiko terhadap *core banking system*, meliputi risiko *downtime*, gangguan jaringan, sistem lambat, keamanan *cloud*, *human error*, dan kepatuhan regulasi.	Prioritas risiko belum ditentukan secara terukur.	Menerapkan Risk Matrix berdasarkan tingkat kemungkinan (*likelihood*) dan dampak (*impact*) untuk menentukan prioritas risiko dan mendukung.
APO12.06 (Respond to risk)	BPR telah memiliki mekanisme respons risiko melalui prosedur penanganan insiden, *failover* jaringan.	Proses respons dan pemulihan insiden belum sepenuhnya cepat, konsisten, dan terstandarisasi	Menyusun Incident Response Playbook dan melakukan incident response drill secara berkala.
DSS01.01 (Perform operational procedures)	BPR telah menerapkan prosedur operasional harian *core banking system* berdasarkan SOP, meliputi *start of day*, monitoring transaksi, pencatatan gangguan, *backup* harian, dan *end of day*.	Pelaksanaan SOP operasional belum sepenuhnya konsisten dan terdokumentasi secara seragam di seluruh unit kerja.	Menerapkan Digital Operational Checklist untuk memastikan setiap prosedur operasional terdokumentasi, terverifikasi.
DSS01.03 (Monitor IT infrastructure)	BPR telah melakukan monitoring infrastruktur *CBS* melalui *dashboard* monitoring dan mekanisme *failover* jaringan.	Monitoring infrastruktur belum mampu mendeteksi dan menangani gangguan secara cepat sehingga sistem lambat, dan *downtime* masih terjadi.	Menerapkan Infrastructure Monitoring Dashboard berbasis *real-time* dengan fitur early warning untuk mempercepat deteksi dan penanganan gangguan.
DSS01.04 (Manage the environment)	BPR telah menerapkan *backup* data harian, memiliki Data Recovery Center (DRC), serta melakukan *disaster recovery drill* untuk mendukung keberlangsungan operasional.	Mekanisme pemulihan layanan belum sepenuhnya optimal.	Meningkatkan monitoring backup dan pengujian DRC secara berkala.
MEA03.01 (Identify external compliance requirements)	BPR telah menerapkan kepatuhan terhadap regulasi melalui audit internal dan eksternal secara berkala serta kebijakan operasional yang mengacu pada ketentuan OJK dan regulator terkait.	Pemahaman dan penerapan persyaratan kepatuhan belum merata di seluruh unit kerja	Menyusun Compliance Monitoring Plan serta melakukan sosialisasi regulasi secara berkala.
MEA03.03 (Confirm external compliance)	BPR telah menindaklanjuti temuan audit melalui rencana aksi perbaikan, penetapan target penyelesaian, dan pelaporan.	Monitoring penyelesaian tindak lanjut audit belum optimal.	Menerapkan Audit Action Tracking untuk memantau progres penyelesaian setiap temuan audit.

Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id
E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

3.1.8 Implementasi ISO 27001:2022

Berdasarkan hasil wawancara dan analisis terhadap kontrol A.5.1 (Information Security Policies), A.5.23 (Information Security for Use of Cloud Services), dan A.5.30 (ICT Readiness for Business Continuity), PT BPR NTB Perseroda telah menerapkan kontrol keamanan informasi yang mendukung operasional core banking system berbasis cloud. Penerapan tersebut meliputi kebijakan keamanan informasi, pengelolaan keamanan layanan cloud, serta mekanisme keberlangsungan layanan seperti backup data, Data Recovery Center (DRC), Business Continuity Plan (BCP), dan disaster recovery drill. Dalam penelitian ini, ISO/IEC 27001:2022 digunakan sebagai acuan untuk mengidentifikasi penerapan kontrol keamanan informasi, bukan untuk melakukan audit sertifikasi atau menilai tingkat kepatuhan organisasi terhadap standar ISO. Oleh karena itu, hasil penelitian menunjukkan bahwa kontrol keamanan informasi telah diterapkan sesuai dengan ruang lingkup penelitian, tanpa menyatakan bahwa organisasi telah tersertifikasi ISO/IEC 27001:2022.

Integrasi COBIT 5 dan ISO/IEC 27001:2022 memberikan evaluasi yang lebih komprehensif dibandingkan penggunaan satu framework saja. COBIT 5 digunakan untuk mengukur tingkat kapabilitas proses tata kelola teknologi informasi melalui Capability Level, sedangkan ISO/IEC 27001:2022 digunakan untuk memverifikasi bahwa proses tersebut telah didukung oleh kontrol keamanan informasi yang relevan. Dengan demikian, hasil evaluasi tidak hanya menunjukkan sejauh mana tata kelola teknologi informasi telah diterapkan, tetapi juga sejauh mana kontrol keamanan informasi mampu mendukung keandalan, keamanan, dan keberlangsungan operasional core banking system. Integrasi kedua framework tersebut menghasilkan rekomendasi yang lebih tepat sasaran karena mencakup aspek tata kelola, manajemen risiko, operasional, kepatuhan, serta penguatan kontrol keamanan informasi secara terpadu.

3.1.9 Pemetaan Keterkaitan COBIT 5 dan ISO 27001:2022

Tabel 7. Integrasi COBIT 5 dan ISO 27001:2022

Domain COBIT 5	Control ISO 27001:2022	Keterkaitan Framework
EDM01 (Ensure Governance Framework Setting and Maintenance)	A.5.1 – Information Security Policies	EDM01 berfokus pada penetapan dan pemeliharaan tata kelola teknologi informasi, termasuk penyusunan kebijakan, pengawasan, dan evaluasi. Kontrol A.5.1 melengkapi domain tersebut dengan memberikan acuan mengenai penyusunan, penerapan, komunikasi, serta peninjauan kebijakan keamanan informasi sebagai bagian dari tata kelola TI.
APO12 (Manage Risk)	A.5.23 – Information Security for Use of Cloud Services	APO12 berfokus pada proses identifikasi, analisis, dan pengelolaan risiko teknologi informasi. Kontrol A.5.23 melengkapi proses tersebut dengan memberikan panduan mengenai pengelolaan keamanan informasi pada penggunaan layanan *cloud*, termasuk pengelolaan risiko, pengawasan terhadap penyedia layanan, serta penerapan pengendalian keamanan pada lingkungan *cloud*.
DSS01 (Manage Operations)	A.5.30 – ICT Readiness for Business Continuity	DSS01 berfokus pada pengelolaan operasional teknologi informasi agar layanan dapat berjalan secara berkelanjutan. Kontrol A.5.30 melengkapi domain tersebut melalui penerapan kesiapan teknologi informasi dalam mendukung keberlangsungan layanan, seperti mekanisme *backup*, *Business Continuity Plan* (BCP), *Data Recovery Center* (DRC), *Recovery Time Objective* (RTO), serta pengujian pemulihan sistem (*disaster recovery drill*).

Jurnal Sistem Komputer (SISKOM)
https://journal.stmiki.ac.id
E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

MEA03 (Monitor, Evaluate and Assess Compliance)	A.5.1 – Information Security Policies	EDM01 berfokus pada penetapan dan pemeliharaan tata kelola teknologi informasi, termasuk penyusunan kebijakan, pengawasan, dan evaluasi. Kontrol A.5.1 melengkapi domain tersebut dengan memberikan acuan mengenai penyusunan, penerapan, komunikasi, serta peninjauan kebijakan keamanan informasi sebagai bagian dari tata kelola TI.

3.2 Pembahasan

Penelitian ini bertujuan untuk mengevaluasi efektivitas tata kelola teknologi informasi (TI) dalam operasional core banking system di PT BPR NTB Perseroda, menggunakan framework COBIT 5 yang didukung oleh kontrol keamanan informasi berdasarkan ISO/IEC 27001:2022. Transformasi industri perbankan yang didorong oleh perkembangan teknologi informasi telah meningkatkan efisiensi operasional, mempercepat layanan, dan meningkatkan akurasi dalam pengelolaan data (Hidayah *et al.,* 2024). PT Bank BPR NTB Perseroda adalah lembaga keuangan yang mengandalkan core banking system berbasis cloud sebagai infrastruktur utama dalam operasionalnya. Ketergantungan yang tinggi terhadap sistem ini menuntut adanya tata kelola TI yang baik untuk memastikan ketersediaan layanan, keandalan sistem, dan keamanan informasi. Hasil observasi dan wawancara dengan Sub Divisi Operasional Teknologi dan Informasi mengungkapkan beberapa kendala, termasuk gangguan pada jaringan layanan cloud, ketidakstabilan pasokan listrik, dan potensi ancaman keamanan siber (Tanjung *et al.,* 2025). Masalah ini berdampak langsung pada keterlambatan proses kredit dan transaksi nasabah, yang dapat merugikan reputasi dan kinerja bank.

Penelitian ini menggunakan pendekatan mixed methods, yang menggabungkan metode kualitatif dan kuantitatif (Negeri *et al.,* 2024). Data dikumpulkan melalui wawancara, observasi, studi dokumentasi, dan kuesioner yang melibatkan 32 responden. Analisis data dilakukan menggunakan Process Assessment Model (PAM) dari COBIT 5. Hasil evaluasi menunjukkan bahwa tata kelola TI berada pada Capability Level 3 (Established Process) dengan rata-rata nilai 3,31 dan gap sebesar 0,69 menuju Level 4 (Predictable Process). Ini menunjukkan bahwa proses tata kelola telah diterapkan secara terdokumentasi dan terstandarisasi, namun pengelolaan risiko dan pemantauan operasional masih perlu ditingkatkan untuk mencapai level yang lebih tinggi (Daffa Iqbal Agselmora & Utomo, 2022). Penerapan kontrol keamanan informasi berdasarkan ISO/IEC 27001:2022 mencakup kebijakan keamanan informasi, pengelolaan keamanan layanan cloud, dan mekanisme keberlangsungan layanan TI (Frangky & Sinaga, 2024). Meskipun kontrol tersebut telah diterapkan, masih ada kebutuhan untuk meningkatkan pengukuran kinerja, monitoring, dan evaluasi proses agar tata kelola TI dapat berjalan lebih terukur dan berkelanjutan (Lestari *et al.,* 2025).

Rekomendasi perbaikan yang diusulkan harus dilaksanakan secara bertahap berdasarkan prioritas domain. Domain DSS01 (Manage Operations) menjadi prioritas utama karena memiliki gap tertinggi dan dampak langsung terhadap operasional core banking system. Langkah selanjutnya adalah fokus pada EDM01 (Ensure Governance Framework Setting and Maintenance) untuk memperkuat mekanisme tata kelola, diikuti oleh APO12 (Manage Risk) untuk meningkatkan pengelolaan risiko TI, serta MEA03 (Monitor, Evaluate and Assess Compliance) untuk mengoptimalkan pemantauan kepatuhan (Hanif *et al.,* 2025).

Hasil penelitian menunjukkan bahwa integrasi COBIT 5 dan ISO/IEC 27001:2022 memberikan evaluasi yang lebih komprehensif terhadap tata kelola dan keamanan informasi (Kristen & Wacana, 2025). Dengan menggunakan kedua framework ini, organisasi dapat memastikan bahwa proses tata kelola TI tidak hanya efektif tetapi juga didukung oleh kontrol keamanan yang relevan. Penelitian ini menyimpulkan bahwa meskipun tata kelola TI telah diterapkan dengan baik, masih ada ruang untuk perbaikan, terutama dalam hal pengelolaan risiko dan pemantauan operasional (Prasetya *et al.,* 2025).

Untuk penelitian selanjutnya, melakukan evaluasi ulang setelah penerapan rekomendasi perbaikan guna menilai peningkatan kapabilitas tata kelola TI. Penelitian berikutnya juga dapat mempertimbangkan penggunaan COBIT 2019 sebagai kerangka kerja pembanding atau

E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

mengevaluasi efektivitas implementasi kontrol keamanan informasi berdasarkan ISO/IEC 27001:2022 setelah perbaikan dilakukan (Nawir *et al.,* 2022).

4. Kesimpulan

Penelitian ini berhasil mengevaluasi efektivitas tata kelola teknologi informasi dalam operasional core banking system PT BPR NTB Perseroda menggunakan framework COBIT 5, didukung oleh kontrol keamanan informasi ISO/IEC 27001:2022. Hasil evaluasi menunjukkan bahwa tata kelola teknologi informasi berada pada Capability Level 3 (Established Process) dengan rata-rata nilai 3,31 dan gap sebesar 0,69 menuju Level 4 (Predictable Process). Hal ini menandakan bahwa proses tata kelola telah diterapkan secara terdokumentasi dan terstandarisasi, serta mampu mendukung operasional core banking system. Penerapan kontrol keamanan informasi berdasarkan ISO/IEC 27001:2022 mencakup kebijakan keamanan informasi, keamanan layanan cloud, dan keberlangsungan layanan TI, yang telah berkontribusi pada pengelolaan keamanan informasi organisasi. Namun, peningkatan masih diperlukan dalam pengukuran kinerja, monitoring, pengelolaan risiko, evaluasi proses, dan penguatan implementasi kontrol keamanan informasi agar tata kelola dapat lebih terukur, terkendali, dan berkelanjutan sesuai karakteristik Level 4. Rekomendasi perbaikan disarankan dilaksanakan secara bertahap berdasarkan prioritas domain. Domain DSS01 (Manage Operations) menjadi prioritas utama karena gap tertinggi dan pengaruh langsung terhadap operasional core banking system. Selanjutnya, fokus pada EDM01 (Ensure Governance Framework Setting and Maintenance) untuk memperkuat tata kelola, diikuti oleh APO12 (Manage Risk) untuk meningkatkan pengelolaan risiko TI, serta MEA03 (Monitor, Evaluate and Assess Compliance) untuk mengoptimalkan pemantauan kepatuhan. Untuk penelitian selanjutnya, disarankan evaluasi ulang setelah implementasi rekomendasi untuk menilai peningkatan kapabilitas tata kelola TI. Penelitian juga dapat mempertimbangkan penggunaan COBIT 2019 sebagai kerangka kerja pembanding untuk evaluasi lebih lanjut.

5. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada PT BPR NTB Perseroda yang telah memberikan izin penelitian serta dukungan selama proses pengumpulan data. Penulis juga menyampaikan penghargaan kepada Bapak Khairan Marzuki, Bapak Andi Sofyan Anas, Bapak Ondi Asroni, dan Bapak Wisnu Alfiansyah atas waktu, bimbingan, masukan, serta informasi yang diberikan selama proses penelitian. Ucapan terima kasih juga disampaikan kepada seluruh narasumber dan responden, baik di Kantor Pusat maupun kantor cabang PT BPR NTB Perseroda, yang telah berpartisipasi dalam wawancara, observasi, dan pengisian kuesioner sehingga penelitian ini dapat diselesaikan dengan baik.

6. Daftar Pustaka

Agselmora, D. I., & Utomo, A. P. (2022). Audit teknologi informasi menggunakan COBIT 5 domain DSS pada Universitas Stikubank Semarang. *Jurnal Teknik Informatika Dan Sistem Informasi, 9*(4), 2804–2814. http://jurnal.

Amiryan Ahadis, M. R., Nama, G. F., Annisa, R., & M. A. M. (2025). Audit tata kelola teknologi informasi menggunakan framework COBIT 5 pada PT Bank Rakyat Indonesia Unit 1 Pringsewu. *Jurnal Informatika Dan Teknik Elektro Terapan, 13*(2), 1454–1462. https://doi.org/10.23960/jitet.v13i2.6477

E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

Forester, B. J., Idris, A., Khater, A., Afgani, M. W., Isnaini, M., Islam, U., Raden, N., & Palembang, F. (2024). Penelitian kuantitatif: Uji reliabilitas. *Quantitative Research: Data Reliability Test, 4*(3), 1812–1820.

Frangky, & Sinaga, R. (2024). Penerapan ISO/IEC 27001:2022 dalam tata kelola keamanan sistem informasi: Evaluasi proses dan kendala. *Nuansa Informatika, 18*(2), 46–54. https://doi.org/10.25134/ilkom.v18i2.205

Gade, U. R. (2025). Core banking system modernization (Retail banking). *Sarcouncil Journal of Multidisciplinary, 5*(9), 112–121.

Hanif, M. F., Harahap, A. R., Fakhrudin, A., Madina, F. F., & Febriawan, D. (2025). Integrating COBIT and ISO frameworks in IT audits: A literature review. *International Journal of Emerging Research in Engineering, Science, and Management, 4*(3), 8–14. https://doi.org/10.58482/ijeresm.v4i3.2

Hidayah, N., Amanda, A., & Az-Jahra, S. (2024). Menelaah tantangan bank syariah dalam menghadapi perkembangan di era digital. *Journal of Waqf and Islamic Economic Philanthropy, 1*(3), 1–8. https://doi.org/10.47134/wiep.v1i3.295

Kristen, U., & Wacana, S. (2025). Penerapan framework COBIT pada perbankan di Indonesia: Sebuah tinjauan literatur sistematis. *10*(3), 2426–2434.

Lestari, P. S., Tambunan, F. Z., Nasution, A. W., Amelia, M., Lita, C., Panjaitan, P., & Sinaga, D. S. (2025). Implementasi ISO 27001 dalam meningkatkan kepercayaan pengguna dalam sektor industri. *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan, 4*(1), 1152–1167.

Nawir, M., Ap, I., & Wajidi, F. (2022). Integrasi framework ISO 27001 dan COBIT 2019 pada keamanan informasi smart tourism PT. YoY Manajemen Internasional. *J-ICON, 10*(2), 122–128. https://doi.org/10.35508/jicon.v10i2.7985

Negeri, U., Thaha, S., Jambi, S., & Kuantitatif-kualitatif, P. (2024). Pendekatan penelitian kuantitatif dan kualitatif serta tahapan penelitian. *15*(1), 82–92.

Prasetya, B., Mahardhika, D. P., & Usino, W. (2025). Analysis of the effect of system quality, information quality, and service quality on user satisfaction of T24 application (Temenos Transact core banking) with perceived usefulness as an intervening variable (case study: J Trust Bank Indonesia). *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE), 8*(3), 7453–7471.

Pratiwi, S. F., Zalukhu, L. A., Tesa, A. R., Aisyah, I. S., & Saputra, B. (2025). Implementasi digital pada tata kelola administrasi: Upaya meningkatkan mutu pelayanan di era birokrasi modern. *2*(June), 38–44.

Pratiwi, Y., & Widianti, L. W. (2025). Implementasi tata kelola teknologi informasi menggunakan framework COBIT 5 pada salah satu bank milik BUMN. *Jurnal Kecerdasan Buatan Dan Teknologi Informasi, 4*(2), 98–113. https://doi.org/10.69916/jkbti.v4i2.281

Ramadhian, P. R., Dwiki, G., Aryono, P., & Masyhuri, M. (2025). Audit of the Srikandi information system at the Banten regional library and archives department using the COBIT 5 framework. *10*(3), 1321–1330.

E-ISSN: 3047-7565 | P-ISSN: 2775-3115
Vol. 6 No. 3 (2026) | Sep
OPEN ACCESS
https://doi.org/10.35870/siskom.v6i3.1973

Tanjung, A. M., Lase, W. A., Zega, O., & Lafau, R. O. (2025). Keamanan siber dalam sistem informasi berbasis cloud: Tantangan dan solusi. *02*, 127–133.

Yoga, T. P., Maharani, V., & Maulana, N. D. (2024). Audit keamanan sistem informasi puskesmas dengan standar ISO/IEC 27001:2013 dan framework COBIT 5. *Nuansa Informatika, 18*(1), 2614–5405. https://journal.fkom.uniku.ac.id/ilkom93

Zayrin, A. A., Nupus, H., Maizia, K. K., & Marsela, S. (2025). Analisis instrumen penelitian pendidikan (uji validitas dan reliabilitas instrumen penelitian). *780–789*.