Analisis Manajemen Risiko Relokasi *Disaster Recovery Center* (DRC) Bank Tabungan Negara, Tbk

Rifa'at Abdul Haziz Muslim[*1], Samsul Arifin[2]
[1]Sistem Informasi, [2]Teknologi Informasi, [12]STMIK PPKIA Pradnya Paramita
Korespondensi: [*]rifa'at25510004@stimata.ac.id

Info Artikel

Diajukan: 22 Juni 2026
Diterima: 30 Oktober 2026
Diterbitkan: 10 November 2026

Keywords:
COBIT 2019; Disaster Recovery Center; IT governance; ISO 31000; IT risk management

Kata Kunci:
COBIT 2019; Disaster Recovery Center; ISO 31000; manajemen risiko TI; tata kelola TI

Check for updates

Lisensi: *cc-by-sa*

Copyright © 2026 Rifa'at Abdul Haziz Muslim, Samsul Arifin

Abstract

The relocation of the Disaster Recovery Center (DRC) is a strategic initiative for banking business continuity, yet it carries operational risks that must be managed carefully. This study analyzes the risk management of the DRC relocation at PT Bank Tabungan Negara, Tbk (BTN) by integrating the ISO 31000:2018 and COBIT 2019 frameworks. A qualitative descriptive method with a case study approach was applied, drawing on interviews and internal assessment documents. Risks were identified, analyzed using a probability and impact matrix, evaluated, and treated through the ISO 31000 stages, while IT governance was assessed through the COBIT 2019 APO12 (Managed Risk) domain. The results reveal four main risks, with the unavailability of network and supporting cabling infrastructure classified as an extreme risk that directly threatens the cut-over phase and the achievement of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets. The governance evaluation shows that the APO12 capability is at Level 3 (Established Process), indicating a coordination gap between IT planning and procurement. The study recommends fast-track procurement, independent quality assurance, and technical cross-review of procurement documents to ensure service resilience and business value.

Abstrak

Relokasi Disaster Recovery Center (DRC) merupakan inisiatif strategis bagi kelangsungan bisnis perbankan, namun menyimpan risiko operasional yang harus dikelola dengan cermat. Penelitian ini menganalisis manajemen risiko relokasi DRC pada PT Bank Tabungan Negara, Tbk (BTN) dengan mengintegrasikan kerangka kerja ISO 31000:2018 dan COBIT 2019. Metode kualitatif deskriptif dengan pendekatan studi kasus digunakan, bersumber dari wawancara dan dokumen asesmen internal. Risiko diidentifikasi, dianalisis menggunakan matriks probabilitas dan dampak, dievaluasi, serta ditangani melalui tahapan ISO 31000, sementara tata kelola TI dinilai melalui domain COBIT 2019 APO12 (Managed Risk). Hasil penelitian mengungkap empat risiko utama, dengan ketiadaan infrastruktur jaringan dan kabel pendukung tergolong risiko ekstrim yang secara langsung mengancam fase cut-over serta pencapaian target Recovery Time Objective (RTO) dan Recovery Point Objective (RPO). Evaluasi tata kelola menunjukkan kapabilitas APO12 berada pada Level 3 (Established Process), yang mengindikasikan adanya celah koordinasi antara perencanaan TI dan unit pengadaan. Penelitian ini merekomendasikan pengadaan jalur cepat, quality assurance independen, serta tinjauan silang teknis dokumen pengadaan untuk menjamin ketahanan layanan dan nilai bisnis.

Cara mensitasi artikel:
R. A. H. Muslim, S. Arifin. "Analisis Manajemen Risiko Relokasi Disaster Recovery Center (DRC) Bank Tabungan Negara, Tbk". *Jurnal Teknologi Informasi: Teori, Konsep, dan Implementasi (JTI-TKI), vol. 17, no. 2, pp. 74-79, Oktober 2026, https://doi.org/10.36382/jti-tki.v17i2.701*

PENDAHULUAN

Sektor perbankan adalah bagian terpenting dari infrastruktur negara yang sangat bergantung pada ketersediaan dan stabilitas sistem teknologi informasi. Tingginya ketergantungan tersebut menyebabkan setiap gangguan terhadap sistem, baik berupa kegagalan teknis, serangan siber, maupun bencana alam, berpotensi menghentikan layanan kritikal sehingga menuntut tersedianya mekanisme pemulihan yang mampu menjaga kelangsungan operasional. Dalam konteks ini, fungsi dari adanya *Disaster Recovery Center* (DRC) adalah untuk meminimalkan kerugian finansial dan *non*-finansial dalam menghadapi gangguan bisnis atau bencana alam yang meliputi fisik dan informasi berupa data penting perusahaan, serta meningkatkan rasa aman di antara *personel*, *supplier*, *investor*, dan *customer* [1]. Di Indonesia, penyelenggaraan layanan perbankan tunduk pada ketentuan Otoritas Jasa Keuangan (OJK), salah satunya diatur dalam POJK No.38/POJK.03/2016, pasal 21 yang menetapkan pusat pemulihan bencana (*Disaster Recovery Center*) harus berada di wilayah Indonesia untuk menjamin kelangsungan operasional [1]. Kewajiban ini semakin diperkuat oleh POJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, yang mengharuskan bank untuk memiliki tata kelola TI yang memadai, termasuk pengelolaan risiko operasional [2]. Implementasi dari regulasi ini menjadikan aset dan infrastruktur TI sebagai faktor yang esensial dalam menjamin kesinambungan dan keamanan layanan perbankan.

Melalui inisiatif *Recommendation & Roadmap DC Optimization & Improvement of IT Disaster Recovery*, PT

Submitted 22 Juni 2026; Revised 20 Oktober 2026; Accepted 20 Oktober 2026

Bank Tabungan Negara, Tbk menunjukkan komitmen proaktifnya untuk meningkatkan ketahanan infrastruktur TI strategisnya. Keputusan strategis ini disetujui melalui Notula Rapat Komite Pengarah Teknologi Informasi (KPTI) No. 72/M/ITPD/SPG/II/2024 tanggal 16 Februari 2024 [3]. Notula ini secara khusus menyetujui *roadmap data center*, yang mencakup implementasi konsep *Data Center* 2N+1 dan rencana pemindahan DRC dari tempat lamanya. Konsep 2N+1 adalah strategi redundansi pusat data yang menyediakan dua sistem independen secara penuh (2N) ditambah satu komponen cadangan (+1); konfigurasi ini bertujuan meminimalkan *single point of failure* dan menjaga ketersediaan layanan (*high availability*) selama terjadi gangguan maupun pemeliharaan terjadwal.

Meskipun relokasi bertujuan untuk meningkatkan kapabilitas (2N+1), proyek ini membawa risiko yang harus dipertimbangkan dengan hati-hati. Data internal menunjukkan bahwa pengadaan DRC terbaru tidak mencakup perangkat *network* dan infrastruktur kabel pendukung. Kondisi ini menciptakan celah risiko operasional yang signifikan, yang dapat memengaruhi *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO) bank. Kegagalan dalam mengelola risiko ini dapat menyebabkan kerugian moneter besar dan kehilangan kepercayaan masyarakat. Selain itu, semakin kompleksnya risiko yang dihadapi bank menuntut penguatan praktik tata kelola perusahaan yang lebih matang [2]. Untuk menjawab berbagai potensi kerugian tersebut, diperlukan penerapan manajemen risiko yang terstruktur guna mengidentifikasi, menganalisis, dan mengendalikan risiko relokasi sejak tahap awal. Penerapan manajemen risiko juga mendukung pengambilan keputusan yang lebih tepat serta peningkatan efisiensi [4]. Manajemen risiko juga berperan dalam meminimalkan terjadinya risiko yang berdampak besar [5]. Hal ini menegaskan bahwa keberhasilan relokasi bergantung pada efektivitas penerapan manajemen risiko.

Berdasarkan latar belakang ini, fokus utama penelitian ini adalah untuk menganalisis manajemen risiko relokasi DRC BTN. Penelitian ini akan mempelajari bagaimana risiko utama diidentifikasi, terutama yang berkaitan dengan celah dalam pengadaan infrastruktur *network* dan kabel pendukung. Selain itu, penelitian ini akan merumuskan usulan penanganan risiko yang sesuai untuk memitigasi celah tersebut. Tujuan akhir dari penelitian ini adalah untuk mengevaluasi seberapa efektif proses manajemen risiko relokasi DRC BTN yang menggunakan pedoman ISO31000 (ISO, 2018) dan COBIT 2019 (ISACA, 2019). Dalam penelitian ini, efektivitas tersebut diukur secara konkret melalui tingkat kapabilitas (*capability level*) proses tata kelola pada domain COBIT 2019, sehingga penelitian dapat memberikan rekomendasi manajerial yang terukur dan berorientasi pada nilai bisnis (*business value*).

METODE

Metode kualitatif deskriptif dan studi kasus digunakan dalam penelitian ini untuk meninjau manajemen risiko pada proyek relokasi *Disaster Recovery Center* (DRC) Bank BTN. Pendekatan ini dipilih karena memungkinkan peneliti mengeksplorasi risiko secara mendalam dan menggambarkan kondisi manajemen risiko berdasarkan fakta nyata di lapangan [5]. Melalui metode ini, peneliti dapat meninjau kebijakan internal, masalah manajerial, dan strategi mitigasi yang tidak dapat diukur secara statistik tetapi berdampak strategis pada kesinambungan bisnis.

A. *Tahapan Penelitian Menurut ISO31000:2018*

Metodologi analisis manajemen risiko penelitian ini menggunakan kerangka kerja sistematis dan terstruktur ISO31000:2018. Prinsip dan pedoman ISO31000:2018 sangat tepat digunakan dan diakui secara internasional. Identifikasi risiko, analisis risiko, evaluasi risiko, dan *risk treatment* (mengusulkan perlakuan untuk mengurangi atau menghilangkan risiko) digunakan sebagai tahapan dalam penelitian ini [6][7].

1) Identifikasi Risiko (*Risk Identification*): Prosedur untuk menemukan, mengenali, dan menjelaskan ancaman yang dapat membantu atau menghambat pencapaian tujuan relokasi DRC. Fokus identifikasi terkonsentrasi pada celah infrastruktur *network* dan kabel pendukung yang ditemukan dalam asesmen internal ITOD (*IT Operation Division*).
2) Analisis Risiko (*Risk Analysis*): Tahapan ini dilakukan untuk memahami sifat risiko dan menentukan tingkat risiko. Setiap risiko dimasukkan ke dalam Matriks Probabilitas dan Dampak (*Probability & Impact Matrix*) untuk melakukan analisis. Skala dampak dihitung berdasarkan kemungkinan gangguan terhadap integritas data dan *Service Level Agreement* (SLA) perbankan.
3) Evaluasi Risiko (*Risk Evaluation*): Menentukan prioritas penanganan dengan membandingkan hasil analisis risiko dengan kriteria risiko yang ditetapkan oleh Bank BTN. Risiko dengan peringkat "Tinggi" atau "Ekstrim" menjadi prioritas utama untuk ditangani.
4) Penanganan Risiko (*Risk Treatment*): Merumuskan usulan penanganan untuk mengurangi atau menghilangkan risiko. Secara konseptual, ISO31000 mengenal empat opsi penanganan, yaitu mitigasi (mengurangi risiko), transfer (melalui asuransi atau vendor), penghindaran, dan penerimaan risiko; pemilihan opsi disesuaikan dengan karakteristik dan tingkat masing-masing risiko.

B. *Menggabungkan Tata Kelola dengan COBIT 2019.*

Hasil analisis risiko selanjutnya dievaluasi dari sisi tata kelola menggunakan COBIT 2019 untuk memperoleh

nilai bisnis (*business value*), khususnya pada domain APO12 (*Managed Risk*). Evaluasi ini dilakukan dengan:

- Pemetaan Komponen Tata Kelola: Mengevaluasi bagaimana kebijakan, struktur organisasi, dan sistem informasi Bank BTN mendukung proses manajemen risiko.
- Penilaian Kapasitas: Untuk mengetahui sejauh mana proses manajemen risiko saat ini telah terstandardisasi dan diukur pada tingkat organisasi menggunakan skala nilai 0–5.

C. *Teknik Pengumpulan dan Analisis Data*

Untuk memastikan bahwa hasilnya valid, dua sumber utama digunakan untuk mengumpulkan dan menganalisis data:

- Data Primer: Untuk mendapatkan informasi tentang tantangan riil di lapangan terkait notula rapat KPTI No.72/M/ITPD/SPG/II/2024, peneliti melakukan wawancara mendalam dengan sejumlah pihak berwenang di Bank BTN, termasuk unit IT *Disaster Recovery* dan manajemen proyek relokasi.
- Data Sekunder: Analisis dokumen internal seperti *Roadmap DC Optimization*, hasil asesmen ITOD, kebijakan tata kelola TI, dan peraturan eksternal seperti POJK Nomor 11/POJK.03/2022 termasuk dalam kategori ini.

D. *Parameter Analisis Manajemen Risiko*

Pendekatan kuantifikasi risiko berbasis parameter probabilitas (*likelihood*) dan dampak (*impact*) merupakan praktik yang umum digunakan dalam penelitian manajemen risiko teknologi informasi karena mampu mengubah data kualitatif (hasil wawancara, observasi, dan dokumen) menjadi prioritas risiko yang objektif dan konsisten [8]. Penggunaan skala ordinal lima tingkat (1-5) dalam penilaian *likelihood* dan *impact* juga banyak direkomendasikan dalam penelitian risiko sistem informasi karena memberikan keseimbangan antara kesederhanaan, kejelasan interpretasi, dan ketepatan pengambilan keputusan manajerial [9][4]. Parameter yang ditetapkan dalam penelitian ini digunakan sebagai instrumen analisis, sehingga ditempatkan pada Bab Metodologi dan menjadi dasar perhitungan tingkat risiko pada Bab Hasil dan Pembahasan.

1) *Parameter Probabilitas Risiko (Likelihood*)

Parameter probabilitas risiko digunakan untuk mengukur tingkat kemungkinan terjadinya suatu risiko selama dan setelah proses relokasi DRC. Penilaian probabilitas didasarkan pada frekuensi kejadian risiko yang diperkirakan dari hasil wawancara dengan pihak terkait, temuan asesmen internal ITOD, serta pengalaman historis proyek TI sejenis. Pendekatan ini sejalan dengan praktik penilaian probabilitas risiko pada implementasi ISO31000 di lingkungan sistem informasi dan infrastruktur TI [8][10].

Tabel 1. Skala Probabilitas Risiko (*Likelihood*)

Skor	Kategori	Deskripsi
1	Sangat Rendah	Risiko hampir tidak pernah terjadi (≤ 5%) dan bersifat insidental
2	Rendah	Risiko jarang terjadi (6–20%), namun masih memungkinkan
3	Sedang	Risiko cukup mungkin terjadi (21–50%) pada kondisi tertentu
4	Tinggi	Risiko sering terjadi (51–80%) selama proses relokasi atau operasional
5	Sangat Tinggi	Risiko hampir pasti terjadi (> 80%) apabila tidak ada pengendalian

Skala probabilitas pada Tabel I diadaptasi dari berbagai penilaian manajemen risiko TI berbasis ISO31000 yang menggunakan pendekatan *likelihood* kuantitatif untuk meningkatkan konsistensi penilaian antar-risiko [8][9].

2) *Parameter Dampak Risiko (Impact*)

Parameter dampak risiko digunakan untuk mengukur besarnya konsekuensi yang ditimbulkan apabila risiko terjadi, khususnya terhadap keberlangsungan layanan TI perbankan. Dalam konteks relokasi DRC, dampak risiko dinilai berdasarkan potensi gangguan layanan kritikal, pencapaian target *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO), serta potensi pelanggaran *Service Level Agreement* (SLA). Penilaian dampak dengan fokus pada layanan kritikal dan kontinuitas bisnis merupakan pendekatan yang lazim digunakan dalam studi risiko infrastruktur TI [4][10].

Tabel 2. Skala Dampak Risiko (*Impact*)

Skor	Kategori	Deskripsi Dampak
1	Sangat Rendah	Gangguan minimal, tidak memengaruhi SLA, RTO, maupun RPO
2	Rendah	Gangguan ringan, masih dalam batas toleransi SLA
3	Sedang	Gangguan sementara, berpotensi menurunkan kinerja layanan TI
4	Tinggi	Gangguan signifikan pada layanan kritikal dan target RTO/RPO
5	Sangat Tinggi	Gangguan besar, downtime berkepanjangan, potensi pelanggaran regulasi dan reputasi

Skala dampak ini disusun agar selaras dengan penelitian manajemen risiko TI yang menekankan keterkaitan langsung antara gangguan teknis dan dampak bisnis organisasi [8][4].

3) *Perhitungan dan Kategori Tingkat Risiko (Risk Level*)

Tingkat risiko ditentukan dengan mengalikan nilai probabilitas dan dampak sebagaimana direkomendasikan dalam penerapan ISO31000 berbasis matriks risiko. Model perhitungan ini banyak digunakan dalam penelitian

risiko sistem informasi karena sederhana, transparan, dan mudah dipahami oleh pemangku kepentingan non-teknis [8][9].

Risk Level = Likelihood × Impact

Tabel 3. Kategori Tingkat Risiko (*Risk Level*)

Nilai Risiko (L × I)	Kategori Risiko	Prioritas Penanganan
1 – 5	Rendah	Dapat diterima, dipantau secara berkala
6 – 10	Sedang	Perlu pengendalian tambahan
11 – 15	Tinggi	Perlu mitigasi segera
16 – 25	Ekstrim	Prioritas utama, wajib tindakan strategis

Klasifikasi tingkat risiko ini digunakan untuk menentukan prioritas evaluasi dan perlakuan risiko. Risiko dengan kategori **Tinggi** dan **Ekstrim** menjadi fokus utama mitigasi, sebagaimana direkomendasikan dalam studi-studi ISO31000 pada sistem informasi kritikal [4][10].

Parameter analisis risiko yang ditetapkan pada subbab ini berfungsi sebagai instrumen penilaian dalam mengukur tingkat risiko relokasi DRC Bank BTN. Seluruh risiko yang teridentifikasi dianalisis menggunakan parameter *likelihood*, *impact*, dan *risk level* untuk menghasilkan kategori prioritas risiko, yang selanjutnya akan dibahas mendalam pada Bab Hasil dan Pembahasan. Pendekatan ini memastikan keterpaduan antara metode analisis dan hasil penelitian, sebagaimana dianjurkan dalam penelitian manajemen risiko teknologi informasi berbasis ISO31000 [8].

III. HASIL DAN PEMBAHASAN

Bagian ini menguraikan hasil implementasi kerangka kerja ISO31000:2018 dan COBIT 2019 dalam menganalisis manajemen risiko proyek relokasi *Disaster Recovery Center* (DRC) Bank Tabungan Negara, Tbk. Analisis difokuskan pada temuan celah pengadaan infrastruktur jaringan dan kabel pendukung yang berpotensi memengaruhi kesinambungan layanan TI secara menyeluruh.

A. Analisis Manajemen Risiko Berdasarkan ISO31000:2018

Penerapan standar ISO31000:2018 diakui secara luas mampu memberikan pedoman struktural yang komprehensif bagi institusi dalam memetakan ketidakpastian operasional sistem TI [6],[7]. Proses manajemen risiko dijalankan melalui empat tahapan utama, yaitu identifikasi, analisis, evaluasi, dan penanganan risiko.

1) Identifikasi Risiko (*Risk Identification*)

Berdasarkan dokumen *Roadmap DC Optimization* serta asesmen internal, identifikasi difokuskan pada celah infrastruktur *network* dan kabel pendukung. Secara teknis, celah tersebut berkaitan langsung dengan kesiapan komponen jaringan inti yang menjadi tulang punggung interkoneksi antar pusat data, sehingga spesifikasi perangkat dan protokol yang digunakan perlu ditinjau secara cermat. Mengingat kompleksitas relokasi pusat data, kesiapan perangkat keras seperti *switch core Cisco Nexus* untuk *data center* dan lini *Catalyst* untuk distribusi menjadi sangat penting. Kegagalan konvergensi *routing protocol* seperti BGP dan OSPF antar *site* dapat terjadi jika infrastruktur fisik belum terpenuhi secara presisi. Berikut adalah daftar risiko utama yang teridentifikasi selama masa transisi relokasi:

- **R1**: Kegagalan pencapaian target operasional DRC akibat tidak tersedianya perangkat jaringan dan infrastruktur kabel pendukung secara tepat waktu.
- **R2**: Kegagalan sinkronisasi dan replikasi data antar *Data Center* dan *Data Center Recovery* baru, yang mengancam pemenuhan *Recovery Point Objective* (RPO).
- **R3**: Terjadinya downtime layanan kritikal di luar *maintenance window*, berpotensi melanggar *Service Level Agreement* (SLA).
- **R4**: Pembengkakan anggaran (*cost overrun*) akibat kebutuhan pengadaan darurat (*emergency procurement*) untuk menutupi celah infrastruktur.

2) Analisis Risiko (*Risk Analysis*)

Risiko yang teridentifikasi kemudian diukur menggunakan parameter *Likelihood* (Probabilitas) dan *Impact* (Dampak). Pengukuran ini penting agar setiap ancaman dapat dikuantifikasi nilai urgensinya sebelum menentukan skala penanganan [8],[5]. Penetapan nilai probabilitas dan dampak pada setiap risiko mengacu pada hasil wawancara dengan unit IT Disaster Recovery dan IT Operation Division (ITOD) serta telaah dokumen asesmen internal, sehingga nilai pada Tabel IV merepresentasikan kondisi aktual proyek dan bukan asumsi semata. Sebagai ilustrasi, R1 memperoleh nilai probabilitas dan dampak yang tinggi (4 dan 4) karena ketiadaan perangkat jaringan inti berdampak langsung pada kegagalan target operasional DRC, sedangkan R2 dinilai berdampak maksimal (5) karena kegagalan replikasi data secara langsung mengancam pemenuhan RPO. Tingkat risiko dihitung dengan mengalikan *Likelihood* dan *Impact*.

Tabel 4. Hasil Analisis Penilaian Risiko Relokasi DRC

Kode Risiko	Probabilitas (*Likelihood*)	Dampak (*Impact*)	Tingkat Risiko	Kategori Risiko
R1	4	4	16	Ekstrim
R2	3	5	15	Tinggi
R3	2	5	10	Sedang
R4	4	3	12	Tinggi

3) Evaluasi Risiko (*Risk Evaluation*)

Evaluasi dilakukan dengan membandingkan hasil tingkat risiko dengan kriteria prioritas penanganan bank. Berdasarkan Tabel IV, risiko R1 masuk dalam kategori Ekstrim dan menjadi prioritas utama. Sementara itu, R2 dan R4 masuk dalam kategori Tinggi, yang membutuhkan mitigasi segera agar fungsi pemulihan bencana tidak terganggu. Hal ini sejalan dengan penelitian Kanantyo dan Papilaya (2021) yang menegaskan bahwa risiko berlevel tinggi pada aset jaringan krusial wajib memiliki rencana penanganan seketika sebelum fase *cut-over* dimulai [11].

4) Penanganan Risiko (*Risk Treatment*)

Mengingat seluruh risiko utama bersifat operasional, kritikal, dan berada dalam kendali langsung bank, strategi mitigasi dipilih sebagai opsi penanganan yang paling sesuai dibandingkan transfer, penghindaran, maupun penerimaan risiko. Untuk meminimalkan dampak ancaman, usulan *risk treatment* dirumuskan sebagai berikut:

- **Mitigasi R1 dan R4**: Mengaktifkan pengadaan jalur cepat (*fast-track procurement*) untuk *network cabling*, atau menggunakan skema *managed services* penyewaan *switch/router* sementara agar topologi jaringan awal tetap dapat terbangun.
- **Mitigasi R2**: Mengamankan RPO dengan menggunakan metode replikasi asinkron sementara dan menjadwalkan sinkronisasi data bertahap pada jam *off-peak*.
- **Mitigasi R3**: Memperketat pengawasan *Change Management* saat proses migrasi dan memastikan tersedianya jalur komunikasi *failover* cadangan.

B. Evaluasi Tata Kelola TI dengan COBIT 2019

Manajemen risiko yang tertata wajib diimbangi dengan proses tata kelola (*governance*) yang mendukung tercapainya tujuan perusahaan. Evaluasi dilakukan menggunakan kerangka kerja COBIT 2019 pada domain APO12 (*Managed Risk*) [12],[13].

1) Pemetaan Komponen Tata Kelola

Dukungan struktural terhadap manajemen risiko di Bank BTN telah difasilitasi oleh Komite Pengarah Teknologi Informasi (KPTI). Namun, insiden terlewatinya perencanaan kabel dan kelengkapan jaringan mengindikasikan adanya celah integrasi informasi antara perencana arsitektur infrastruktur TI dan divisi *procurement*. Kebijakan harus disesuaikan agar mewajibkan *cross-review* teknis dokumen pengadaan sebelum proyek disetujui, sesuai dengan prinsip tata kelola yang terintegrasi pada COBIT 2019.

2) Penilaian Kapasitas (*Capability Level*)

Pengukuran pada domain APO12 menunjukkan bahwa kapabilitas manajemen risiko relokasi DRC berada pada Level 3 (*Established Process*). Pada fase ini, prosedur identifikasi dan mitigasi telah terdefinisi dan didokumentasikan dengan baik. Akan tetapi, bank belum mencapai Level 4 (*Predictable Process*), karena belum menerapkan pengukuran kuantitatif prediktif untuk mendeteksi *blind-spot* kebutuhan operasional sejak dini [12]. Temuan ini sejalan dengan studi Hermawan [14] pada infrastruktur jaringan teknologi informasi perbankan, yang turut menempatkan domain APO12 pada Level 3 dan menegaskan bahwa peningkatan tingkat kapabilitas menuntut pengukuran kinerja tata kelola yang lebih terukur.

C. Rekomendasi Manajerial dan Business Value

Integrasi evaluasi ISO31000:2018 dan COBIT 2019 memberikan pandangan yang menyeluruh bagi Bank BTN. Secara operasional, manajemen harus segera mengeskalasi pengadaan darurat infrastruktur pendukung demi kelancaran konvergensi sistem DRC. Kesiapan infrastruktur pusat data tersebut merupakan prasyarat utama keberhasilan rencana pemulihan bencana, sebagaimana ditegaskan Sari dan Ramli [15] melalui perancangan Disaster Recovery Plan pada pusat data instansi. Secara strategis, diperlukan *Quality Assurance* (QA) independen pada tahap perencanaan awal infrastruktur TI di masa depan untuk memastikan *business value*, yaitu efisiensi biaya proyek jangka panjang dan ketersediaan layanan perbankan yang tangguh, dapat tercapai.

IV. KESIMPULAN DAN SARAN

Berdasarkan analisis manajemen risiko dan tata kelola TI pada proyek relokasi *Disaster Recovery Center* (DRC) PT Bank Tabungan Negara, Tbk (BTN), integrasi kerangka kerja ISO31000:2018 dan COBIT 2019 terbukti komprehensif dalam memetakan kesiapan operasional sekaligus mengevaluasi kelemahan struktural. Melalui pendekatan ISO31000:2018, temuan utama menyoroti adanya celah kritis pada pengadaan infrastruktur jaringan (*network*) dan kabel pendukung. Keterlambatan penyediaan perangkat vital ini teridentifikasi sebagai risiko tingkat ekstrim yang secara langsung mengancam kelancaran fase *cut-over*, serta berpotensi menggagalkan pemenuhan target *Recovery Point Objective* (RPO) dan *Recovery Time Objective* (RTO). Di sisi lain, hasil evaluasi tata kelola menggunakan COBIT 2019 pada domain APO12 (*Managed Risk*) menunjukkan bahwa bank telah berada pada Level 3 (*Established Process*). Prosedur mitigasi sejatinya telah terdefinisi dan terdokumentasi dengan baik, namun insiden terlewatinya pengadaan komponen jaringan ini mengindikasikan masih adanya kelemahan koordinasi antara divisi perencana strategis TI dan unit pengadaan (*procurement*).

Penelitian ini masih memiliki keterbatasan sehingga membuka peluang bagi pengembangan pada studi berikutnya. Pertama, integrasi kerangka kerja ISO31000:2018 dan COBIT 2019 dapat diterapkan pada objek yang lebih luas, misalnya bank atau institusi keuangan lain, guna menguji konsistensi dan generalisasi temuan pada konteks yang berbeda. Kedua, penelitian berikutnya disarankan mengembangkan pengukuran risiko kuantitatif yang bersifat prediktif, seperti pemodelan Monte Carlo atau metode FMEA, sebagai upaya mendorong kapabilitas tata kelola dari Level 3 (*Established Process*) menuju Level 4 (*Predictable Process*). Ketiga, cakupan evaluasi tata kelola dapat diperluas dengan melibatkan domain COBIT 2019 lain di luar APO12 atau membandingkannya dengan kerangka kerja lain seperti NIST dan ITIL agar diperoleh penilaian tata kelola TI yang lebih menyeluruh. Terakhir, studi lanjutan dapat melakukan validasi empiris secara longitudinal setelah implementasi untuk mengukur efektivitas penanganan risiko yang diusulkan terhadap pencapaian *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO) yang aktual.

REFERENSI

[1] Otoritas Jasa Keuangan, *Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*. Jakarta: OJK, 2016. [Daring]. Tersedia: https://ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum.aspx

[2] Otoritas Jasa Keuangan, *Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum*. Jakarta: OJK, 2022. [Daring]. Tersedia: https://ojk.go.id/id/regulasi/Documents/Pages/Penyelenggaraan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%2011%20-%2003%20-%202022.pdf

[3] Bank Tabungan Negara, *Notula Rapat Komite Pengarah Teknologi Informasi (KPTI) No. 72/M/ITPD/SPG/II/2024 tentang Roadmap Data Center*. Jakarta: Bank BTN, 2024.

[4] F. F. Akhmad dan Ilham, "Risk Management in Optimizing the Success of Information Technology Projects Using the ISO 31000 Framework," *Jurnal Telematika*, vol. 19, no. 2, 2024.

[5] I. W. A. Juliantara, W. E. Ariawan, dan I. N. A. Guna, "Analisis Manajemen Risiko Sistem Informasi dalam Penggunaan Aplikasi E-Purchasing Berbasis ISO 31000 (Studi Kasus Toko Asha)," *Jurnal Sutasoma*, vol. 3, no. 2, hlm. 51–60, 2025.

[6] F. M. R. M. Junior dan J. J. C. Tambotoh, "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2018 pada INLISlite di Dinas Perpustakaan dan Kearsipan Kota Salatiga," *Jurnal Informatika dan Sistem Informasi*, vol. 17, no. 1, 2025.

[7] M. Aprikasari, L. Benedicta, N. A. Adrielvino, dan A. T. Ayunda, "Penerapan ISO 31000:2018 untuk Manajemen Risiko IT pada Sistem Penerbitan PT. X," *Jurnal Informasi, Sains dan Teknologi*, vol. 7, no. 2, hlm. 154–167, 2024.

[8] R. P. Amzar dan N. Legowo, "Risk-Based Evaluation of Hospital Management Information System Implementation Using ISO 31000 Framework," *Jurnal Ilmiah Manajemen Kesatuan*, vol. 13, no. 6, hlm. 5179–5190, 2025.

[9] S. Hardianti dan I. Riadi, "Service Risk Assessment Learning Management System Using ISO 31000:2018/31010," *International Journal of Computer Applications*, vol. 184, no. 4, hlm. 1–11, 2022.

[10] M. H. Putri, "Information Technology Asset Risk Management Using ISO 31000:2018 Integrated with FMEA," *JEISBI (Journal of Emerging Information System and Business Intelligence)*, Universitas Negeri Surabaya, 2025.

[11] P. Kanantyo dan F. S. Papilaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 8, no. 4, hlm. 1896–1908, 2021.

[12] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL, USA: ISACA, 2018.

[13] R. A. Sari dan Juwairiah, "Evaluation of IT Risk Management in DISKOMINFO of Magelang Regency Using COBIT 2019 Framework Objective EDM03 & APO12," *Telematika: Jurnal Informatika dan Teknologi Informasi*, vol. 20, no. 3, hlm. 442–456, 2023.

[14] S. D. Hermawan, "Evaluasi Capability Level Infrastruktur Jaringan TI Bank XYZ Menggunakan COBIT 2019," *Syntax Literate: Jurnal Ilmiah Indonesia*, vol. 7, no. 12, 2022.

[15] S. W. Sari dan K. Ramli, "Perancangan Disaster Recovery Plan pada Pusat Data dan Teknologi Informasi Komunikasi Instansi XYZ," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 4, hlm. 929–938, 2024.