JURNAL TEKNIK INFORMATIKA DAN MULTIMEDIA Vol 6, No.1, Mei 2026, pp. 121 - 132
p-ISSN : 2808-909X (print)
e-ISSN : 2798-2505 (online)
http://journal.politeknik-pratama.ac.id/index.php/JTIM · page 121
DOI : https://doi.org/10.51903/informatika.v6i1.1529

EVALUASI RISIKO TI PT. KLM MENGGUNAKAN COBIT 5.0 DOMAIN APO12

Septia Angelika Gettin Daely[1*], Chintia Cantika[2], Agnes Elsye Permata Sari[3], Sri Andayani[4]
[1] Universitas Katolik Musi Charitas
Jalan Bangau No. 60 Kota Palembang, e-mail: septiaangelika13@gmail.com
[2] Universitas Katolik Musi Charitas
Jalan Bangau No. 60 Kota Palembang, e-mail: chintiacantikacamn@gmail.com
[3] Universitas Katolik Musi Charitas
Jalan Bangau No. 60 Kota Palembang, e-mail: agneselsye3@gmail.com
[4] Universitas Katolik Musi Charitas
Jalan Bangau No. 60 Kota Palembang, e-mail: andayani_s@ukmc.ac.id
[*] coresspondence

ARTICLE INFO

Article history:

Received 3 December 2025
Received in revised form 13 April 2026
Accepted 20 Mei 2026
Available online 20 Mei 2026

ABSTRACT

This study assesses IT risk management capability at PT. KLM using COBIT 5.0 APO12. Current capability (As-Is) is level 3 (Established Process), with consistent but incomplete documentation and integration, while target capability (To-Be) is level 5 (Optimising Process). The gap highlights the need for better documentation, monitoring, data integration, and automated evaluation. The recommendations include the development of formal documentation, the creation of a standard risk matrix, and the improvement of evaluation mechanisms to support more effective risk management.

Keywords: APO12, capability level, COBIT 5.0.

Abstrak

Penelitian ini menilai kapabilitas manajemen risiko TI PT. KLM menggunakan domain APO12 COBIT 5.0. Hasil menunjukkan *As-Is* berada pada level 3 (*Established Process*) dengan proses yang konsisten namun belum terdokumentasi dan terintegrasi sepenuhnya, sedangkan *To-Be* ditargetkan level 5 (*Optimising Process*). Kesenjangan mencerminkan perlunya peningkatan dokumentasi, pemantauan, integrasi data, dan evaluasi otomatis. Rekomendasi yang dihasilkan mencakup penyusunan dokumentasi formal, pembentukan matriks risiko baku, serta peningkatan mekanisme evaluasi untuk mendukung pengelolaan risiko yang lebih optimal.

Kata Kunci: APO12, COBIT 5.0, level kapabilitas.

Received December 3, 2025; Accepted Mei 20, 2026; Available online Mei 20, 2026

p-ISSN : 2808-909X e-ISSN : 2798-2505

1. PENDAHULUAN

Pemanfaatan teknologi informasi (TI) telah menjadi bagian penting dalam mendukung operasional dan strategi bisnis organisasi modern. Penggunaan TI yang semakin luas membawa peluang sekaligus risiko, mulai dari gangguan sistem, serangan siber, kesalahan prosedural, hingga kegagalan infrastruktur. Tanpa mekanisme manajemen risiko yang terstruktur, organisasi cenderung melakukan penanganan risiko secara reaktif dan tidak konsisten sehingga dapat menghambat pencapaian tujuan bisnis [1]. Berbagai studi menunjukkan bahwa kurangnya dokumentasi formal, lemahnya kontrol internal, dan tidak adanya mekanisme pemantauan berkelanjutan menjadi penyebab utama rendahnya tingkat kematangan manajemen risiko pada banyak organisasi, baik pada sektor pemerintahan maupun layanan publik [1][2].

Kerangka kerja COBIT 5.0 hadir sebagai panduan komprehensif untuk memastikan tata kelola TI berjalan selaras dengan tujuan organisasi. Dengan cakupan proses *end-to-end*, COBIT 5.0 membantu organisasi mengoptimalkan nilai TI, meningkatkan akuntabilitas, serta memperkuat mekanisme pengendalian internal [3]. Dalam konteks manajemen risiko, domain APO12 (*Manage Risk*) menjadi acuan utama untuk melakukan identifikasi, analisis, evaluasi, mitigasi, serta pemantauan risiko TI secara sistematis. Berbagai penelitian menegaskan bahwa penerapan APO12 dapat membantu organisasi memahami posisi kapabilitas saat ini, mengidentifikasi gap proses, serta menyusun rekomendasi peningkatan tata kelola risiko [4][5][6].

PT. KLM merupakan perusahaan yang bergerak dalam pengembangan dan implementasi solusi TI dengan struktur organisasi yang mencakup direktur, *human resource*, *project manager*, *data analyst*, *developer*, hingga *quality assurance*. Sebagai perusahaan yang mengelola layanan berbasis teknologi dan data, risiko TI menjadi bagian penting yang harus dikendalikan secara konsisten. Hasil wawancara dengan unit TI menunjukkan bahwa perusahaan menghadapi beberapa risiko utama seperti serangan siber, *bug* perangkat lunak, risiko kepatuhan, serta risiko operasional terkait pengelolaan sistem. Proses identifikasi risiko dilakukan melalui *workshop*, *threat modelling*, dan *review* insiden terdahulu, dengan acuan COBIT 2019 dan kerangka manajemen risiko internal.

Meskipun proses manajemen risiko telah berjalan, hasil wawancara mengungkapkan bahwa beberapa aspek belum optimal. Identifikasi dan penilaian risiko masih didominasi pendekatan kualitatif, keterlibatan unit non-TI sangat terbatas, dan koordinasi risiko lintas unit belum berjalan efektif. Selain itu, meskipun terdapat monitoring dan laporan rutin, integrasi risiko TI dengan risiko organisasi belum sepenuhnya terdokumentasi. Temuan ini menunjukkan adanya kebutuhan untuk menilai tingkat kematangan manajemen risiko TI secara lebih struktural sesuai kerangka COBIT 5.0, khususnya pada domain APO12.

Berdasarkan kondisi tersebut, penelitian ini dilakukan untuk mengevaluasi tingkat kapabilitas proses manajemen risiko TI PT. KLM menggunakan domain APO12 COBIT 5.0. Penelitian ini diharapkan dapat memberikan gambaran menyeluruh terkait kesenjangan proses yang ada, serta menghasilkan rekomendasi perbaikan yang dapat mendukung ketahanan, keandalan, dan efektivitas pengelolaan risiko TI di perusahaan.

2. TINJAUAN PUSTAKA

2.1. Manajemen Risiko

Manajemen risiko merupakan proses terstruktur untuk mengidentifikasi, menilai, dan mengendalikan berbagai potensi ancaman yang dapat menghambat tujuan organisasi. Dalam konteks teknologi informasi, pengelolaan risiko menjadi semakin penting karena penggunaan TI menghadirkan berbagai potensi gangguan seperti serangan siber, kelemahan sistem, kesalahan prosedural, dan ketidakcukupan dokumentasi. Tanpa proses manajemen risiko yang baik, organisasi cenderung menjalankan pengamanan secara reaktif dan tidak konsisten [1].

Penelitian yang dilakukan pada sektor pemerintahan menunjukkan bahwa risiko sering kali muncul akibat kurangnya prosedur formal, tidak adanya standar pengelolaan, serta terbatasnya sumber daya dalam

p-ISSN : 2808-909X e-ISSN : 2798-2505

mengamankan informasi. Meskipun proses sudah berjalan, banyak kegiatan belum terdokumentasi dan belum didukung mekanisme pemantauan berkelanjutan sehingga tingkat kematangan proses masih berada pada kategori rendah hingga menengah [1]. Kondisi serupa ditemukan pada sektor jasa, di mana kesenjangan antara tingkat pengelolaan TI saat ini dan tingkat yang diharapkan menunjukkan perlunya penguatan kebijakan, peningkatan instrumen pengendalian, dan perbaikan dokumentasi [2].

Pada industri pertahanan dan sektor dengan lingkungan teknologi yang kompleks, manajemen risiko TI memiliki peran strategis untuk memastikan keberlangsungan operasional. Penelitian menunjukkan bahwa ketidakjelasan strategi mitigasi, kurangnya efektivitas identifikasi risiko, serta belum optimalnya keterhubungan antara risiko bisnis dan risiko TI dapat menghambat proses pengambilan keputusan. Analisis menggunakan kerangka COBIT 2019 memperlihatkan bahwa beberapa proses dalam domain risiko masih memiliki kesenjangan signifikan dan membutuhkan fokus perbaikan [4].

Studi lainnya menegaskan bahwa risiko TI, seperti kerusakan data, penyalahgunaan akses, kegagalan infrastruktur, dan gangguan aplikasi, dapat berdampak langsung pada efisiensi proses bisnis. Evaluasi tingkat kapabilitas domain APO12 menunjukkan bahwa perusahaan perlu meningkatkan pengelolaan risiko agar lebih proaktif dan terukur, sehingga potensi kerugian dapat diminimalkan dan efektivitas proses bisnis dapat ditingkatkan [5].

Secara keseluruhan, literatur menekankan bahwa manajemen risiko TI bukan hanya mekanisme perlindungan, tetapi juga bagian penting dari tata kelola organisasi modern. Proses ini membantu organisasi menjaga kesinambungan operasional, meningkatkan keandalan informasi, serta memastikan bahwa pengambilan keputusan didasarkan pada pemahaman risiko yang komprehensif.

2.2. COBIT 5.0

COBIT 5.0 adalah kerangka kerja komprehensif yang dikembangkan oleh ISACA untuk membantu organisasi dalam memastikan tata kelola dan manajemen teknologi informasi berjalan selaras dengan tujuan bisnis. Kerangka ini menyediakan prinsip-prinsip, model proses, serta panduan umum yang dapat digunakan untuk mengendalikan, mengukur, dan meningkatkan kinerja TI dalam berbagai konteks organisasi [3]. COBIT 5.0 dirancang untuk menjembatani kebutuhan bisnis terhadap informasi dengan praktik pengelolaan TI yang efektif, sehingga membantu perusahaan menciptakan nilai tambah melalui penggunaan TI yang optimal.

Sebagai kerangka kerja tingkat *enterprise*, COBIT 5.0 mengintegrasikan berbagai standar, praktik terbaik, dan pedoman internasional. Kerangka ini menawarkan pendekatan menyeluruh (*end-to-end*) yang mencakup keseluruhan proses organisasi, tidak hanya fungsi TI. Dengan demikian, COBIT 5.0 dapat digunakan sebagai alat bantu dalam menilai kematangan proses, meningkatkan efektivitas pengendalian internal, serta memastikan bahwa setiap aktivitas TI mendukung sasaran strategis organisasi [3].

Dalam konteks manajemen risiko, COBIT 5.0 menyediakan domain dan proses khusus yang bertujuan untuk mengidentifikasi, menilai, serta mengendalikan risiko TI secara terstruktur. Penelitian sebelumnya menegaskan bahwa COBIT 5.0 merupakan acuan yang banyak digunakan untuk mengevaluasi kapabilitas manajemen risiko, khususnya melalui domain APO12 yang secara langsung berfokus pada proses identifikasi dan mitigasi risiko TI. Domain APO12 (*Manage Risk*) dalam COBIT 5.0 merupakan bagian dari area *Align*, *Plan*, and *Organize* yang berfokus pada bagaimana organisasi mengidentifikasi, menilai, memantau, dan merespons risiko teknologi informasi secara terstruktur. Tujuan utama APO12 adalah memastikan bahwa risiko TI dikelola secara konsisten sehingga mendukung pencapaian tujuan bisnis dan mengurangi potensi gangguan operasional. Proses ini mencakup beberapa aktivitas penting, seperti identifikasi risiko, analisis dampak, evaluasi tingkat kemungkinan kejadian, penentuan respons risiko yang tepat, serta pemeliharaan profil risiko yang diperbarui secara berkala [3].

p-ISSN : 2808-909X e-ISSN : 2798-2505

Penerapan APO12 telah banyak dibahas dalam berbagai penelitian. Meilinda *et al.* (2025) melakukan evaluasi manajemen risiko TI pada perusahaan otomotif dan menemukan bahwa risiko yang sering muncul berkaitan dengan gangguan infrastruktur, kesalahan manusia, serta faktor lingkungan. Penelitian tersebut menunjukkan bahwa organisasi berada pada level 3 (*Established Process*) dengan target menuju level 5, sehingga diperlukan perbaikan pada praktik pengendalian dan tata kelola risiko agar lebih berkelanjutan [8]. Temuan ini menunjukkan bahwa domain APO12 membantu perusahaan melakukan penilaian yang lebih menyeluruh terhadap risiko TI, serta menyediakan dasar untuk menyusun rekomendasi peningkatan tata kelola.

Penelitian lain oleh Budiono *et al.* (2021) pada perusahaan daerah air minum menunjukkan bahwa penilaian kapabilitas pada APO12 juga berada pada level 3, dengan adanya *gap* menuju level yang ditargetkan organisasi. Analisis *capability level* dan *risk assessment* digunakan untuk melihat apakah pengendalian yang ada telah memadai dalam menurunkan kemungkinan dan dampak risiko. Hasil penelitian tersebut menekankan bahwa penerapan APO12 membantu perusahaan memahami area risiko yang belum tertangani secara optimal serta memberikan arahan perbaikan yang harus dilakukan [9].

Selain itu, studi yang dilakukan oleh Fatimah dan Ichwani (2021) menunjukkan bahwa beberapa organisasi masih berada pada tingkat dasar dalam penerapan APO12. Pada kasus PT GBE, level kapabilitas APO12 berada pada level 1 (*Performed Process*) dengan target mencapai level 2. Hasil ini menggambarkan bahwa perusahaan perlu meningkatkan dokumentasi pengelolaan risiko, memperkuat analisis risiko masa depan, melakukan pemisahan tugas, serta membentuk tim khusus untuk manajemen risiko dan keamanan [10]. Temuan tersebut menguatkan bahwa domain APO12 dapat menjadi alat evaluasi yang efektif untuk melihat kematangan tata kelola risiko TI di berbagai jenis organisasi.

Penerapan COBIT 5.0 pada berbagai studi kasus menunjukkan bahwa kerangka ini mampu membantu organisasi memahami titik lemah dalam pengelolaan risiko serta memberikan dasar yang kuat untuk penyusunan rekomendasi perbaikan [6]. Secara keseluruhan, domain APO12 menjadi acuan penting dalam memastikan bahwa organisasi memiliki mekanisme pengelolaan risiko TI yang sistematis, terdokumentasi, dan berorientasi pada perbaikan berkelanjutan. Penerapannya memungkinkan organisasi memahami posisi kapabilitas saat ini, mengidentifikasi *gap*, serta menyusun rekomendasi strategis untuk meningkatkan ketahanan dan keandalan sistem informasi organisasi.

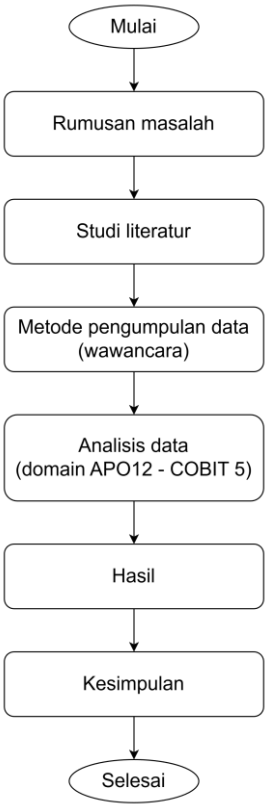
Selain itu, keberlanjutan pengembangan dan penerapan COBIT juga terlihat dari hadirnya versi terbaru (COBIT 2019), yang tetap mempertahankan prinsip inti namun memperbarui struktur agar lebih relevan dengan kebutuhan organisasi modern. Studi terkait menunjukkan bahwa kerangka COBIT tetap menjadi rujukan utama untuk tata kelola TI karena mampu dipetakan dan disesuaikan dengan standar nasional maupun internasional, termasuk dalam bidang pendidikan, industri, dan sektor bisnis lainnya [7].

3. METODOLOGI PENELITIAN

3.1 Kerangka Penelitian

Kerangka penelitian ini disusun untuk memberikan gambaran sistematis mengenai tahapan yang dilakukan dalam menganalisis manajemen risiko TI menggunakan COBIT 5.0 domain APO12 pada PT KLM. Alur penelitian tersebut dapat dilihat pada gambar berikut.

p-ISSN : 2808-909X e-ISSN : 2798-2505



Gambar 3.1 Kerangka Penelitian

3.2 Analisis Domain APO12

Domain APO12 (*Manage Risk*) merupakan bagian dari COBIT 5.0 yang berfokus pada pengelolaan risiko TI secara sistematis. Pada penelitian ini, analisis dilakukan menggunakan enam sub-proses yang terdapat pada APO12. Setiap subdomain digunakan untuk menilai kesesuaian proses perusahaan terhadap standar COBIT 5.0.

3.2.1 APO12.01 (*Collect Data*)

Sub-proses ini berfokus pada pengumpulan informasi yang berhubungan dengan risiko TI. Data tersebut mencakup daftar aset TI, potensi ancaman, kerentanan, insiden sebelumnya, serta faktor lingkungan internal maupun eksternal. Tujuan tahap ini adalah memastikan bahwa semua informasi yang relevan tersedia sebagai dasar untuk identifikasi risiko.

3.2.2 APO12.02 (*Analyze Risk*)

Tahap ini mencakup kegiatan mengidentifikasi risiko, menentukan penyebab, memetakan dampak, dan menilai kemungkinan terjadinya risiko. Proses ini biasanya menghasilkan *risk register* awal yang menggambarkan berbagai risiko yang dapat mengganggu proses bisnis perusahaan.

3.2.3 APO12.03 (*Maintain a Risk Profile*)

Pada tahap ini, seluruh hasil identifikasi dan analisis risiko disusun dalam bentuk profil risiko. Profil ini berisi daftar risiko utama, tingkat keparahan, prioritas penanganan, serta pihak yang bertanggung jawab. Profil risiko harus diperbarui secara berkala agar dapat mencerminkan kondisi terkini perusahaan.

p-ISSN : 2808-909X e-ISSN : 2798-2505

3.2.4 APO12.04 (*Articulate Risk*)
Sub-proses ini memastikan bahwa informasi risiko dapat dikomunikasikan secara jelas kepada pemangku kepentingan yang relevan. Risiko yang telah dianalisis harus dibuat dalam bentuk laporan yang mudah dipahami oleh manajemen, sehingga dapat digunakan dalam pengambilan keputusan.

3.2.5 APO12.05 (*Define a Risk Management Action Portfolio)*
Tahap ini menentukan pilihan tindakan untuk merespons risiko, seperti menghindari, mengurangi (mitigasi), memindahkan (transfer), atau menerima risiko. *Output* yang dihasilkan biasanya berupa daftar rencana mitigasi lengkap dengan prioritas dan estimasi sumber daya yang diperlukan.

3.2.6 APO12.06 (*Respond to Risk*)
Sub-proses terakhir ini meliputi pelaksanaan tindakan yang telah direncanakan untuk menangani risiko. Implementasi dapat berupa penguatan kontrol TI, peningkatan prosedur operasional, pembentukan tim khusus, atau penyediaan mekanisme keamanan tambahan. Keberhasilan tahap ini menjadi dasar untuk menilai efektivitas pengelolaan risiko TI di perusahaan.

3.2.7 Tingkat Kapabilitas
Tingkat kapabilitas dilakukan dengan mengacu pada *Process Capability Model* COBIT 5.0 yang memiliki enam level, mulai dari proses yang belum terlaksana hingga proses yang telah berjalan secara optimal. Evaluasi dilakukan dengan mencocokkan hasil observasi, wawancara, serta bukti pendukung pada masing-masing subproses APO12.01–APO12.06. Nilai yang diperoleh menggambarkan kondisi aktual (*as-is*) dan kemudian dibandingkan dengan level tujuan (*to-be*) yang ingin dicapai oleh organisasi. Perbandingan tersebut menjadi dasar identifikasi kesenjangan serta penyusunan rekomendasi perbaikan.
Berikut rentang level kapabilitas yang digunakan dalam penelitian ini:

Tabel 1. Level Kapabilitas COBIT 5.0

Rentang Nilai	Level	Nilai Kapabilitas	Tingkat Kapabilitas
0 – 0,50	0	0,00	*Non-Existent*
0,51 – 1,50	1	1,00	*Performed Process*
1,51 – 2,50	2	2,00	*Managed Process*
2,51 – 3,50	3	3,00	*Established Process*
3,51 – 4,50	4	4,00	*Predictable Process*
4,51 – 5,00	5	5,00	*Optimising Process*

Nilai kapabilitas dihitung dengan rumus pada persamaan 1 berikut:
NK = Jumlah skor pertanyaan / Jumlah Pertanyaan
Rumus ini digunakan untuk menentukan tingkat kapabilitas pada kondisi *as-is* maupun *to-be*.

4. HASIL DAN PEMBAHASAN

4.1 *Collect Data* (APO12.01)

Berdasarkan hasil wawancara dengan unit TI PT. KLM, proses pengumpulan data risiko dilakukan melalui *workshop* manajemen risiko, *threat modelling*, serta review insiden historis. Identifikasi risiko sepenuhnya dilakukan oleh unit TI, sedangkan unit non-TI belum terlibat dalam proses ini.
Berikut adalah rangkuman risiko yang teridentifikasi pada tahap APO12.01:

Tabel 2. Pengumpulan Data Risiko

No.	Kategori Risiko	Deskripsi Risiko yang Teridentifikasi	Dampak Potensial
1.	Keamanan Siber	Serangan *malware*, *phishing*, dan potensi serangan DDoS terhadap sistem perusahaan	Gangguan layanan, pencurian data, *downtime* operasional, kerugian reputasi

p-ISSN : 2808-909X e-ISSN : 2798-2505

2.	Operasional	*Bug* perangkat lunak pada aplikasi internal maupun produk yang digunakan klien	Gangguan proses kerja, kesalahan output, terhambatnya layanan kepada pengguna
3.	Kepatuhan	Risiko pelanggaran privasi data dan ketidaksesuaian dengan peraturan pemerintah terkait pengelolaan TI dan data	Sanksi hukum, denda, kehilangan kepercayaan pelanggan
4.	Infrastruktur TI	Gangguan pada server, penyimpanan data, atau jaringan yang dapat memengaruhi performa sistem (berdasarkan *review* insiden)	Sistem tidak tersedia, kehilangan data, keterhentian layanan
5.	Perubahan Sistem	Risiko akibat implementasi teknologi baru tanpa analisis dampak yang memadai	Kegagalan integrasi sistem, gangguan operasional, kerentanan baru
6.	*Human Error*	Kesalahan prosedural dalam konfigurasi, *deployment* aplikasi, atau pemeliharaan sistem (disebutkan dari insiden historis)	Kesalahan konfigurasi, celah keamanan, gangguan aplikasi

4.2 *Analyze Risk* (APO12.02) dan *Maintain a Risk Profile* (APO

Pada PT. KLM, risiko dianggap prioritas tinggi apabila dapat mengancam keamanan data, mengganggu operasional inti, atau tidak memiliki kontrol pengendalian yang memadai. Proses analisis dilakukan oleh unit TI melalui penilaian internal, *review* insiden sebelumnya, serta diskusi teknis menggunakan metode *threat modelling*. Pembaruan penilaian risiko dilakukan minimal sekali setiap tahun, atau lebih cepat apabila ada teknologi baru yang akan diimplementasikan. Setelah proses pengumpulan data dan analisis risiko dilakukan, tahap selanjutnya adalah menyusun serta memelihara profil risiko. Tahap ini bertujuan untuk memastikan bahwa setiap risiko yang telah diidentifikasi memiliki tingkat prioritas yang jelas, terdokumentasi dengan baik, dan dapat digunakan sebagai dasar dalam penentuan langkah mitigasi berikutnya. Profil risiko disusun dengan mempertimbangkan peluang terjadinya serta besarnya dampak yang mungkin ditimbulkan, sehingga menghasilkan penetapan tingkat risiko secara konsisten.

Berdasarkan hasil wawancara dan data yang dikumpulkan pada tahap APO12.01, berikut adalah analisis awal tingkat risiko pada perusahaan:

Tabel 3. Analisis Risiko

No.	Risiko	Pengendalian	Peluang	Dampak	Tingkat Risiko
1	Serangan Siber terhadap sistem (*malware*, *phishing*, DDoS)	Penerapan *firewall* berlapis, sistem deteksi ancaman, *antivirus* ter-*update*, pemantauan *log real-time*, serta prosedur penanganan insiden yang sudah terstruktur.	Sedang	Sangat Besar	Tinggi
2	*Bug* atau kesalahan pada aplikasi internal	Proses QA *testing*, review kode rutin, pengujian sebelum rilis, serta dokumentasi perubahan untuk mencegah kesalahan berulang.	Sedang	Besar	Sedang

p-ISSN : 2808-909X e-ISSN : 2798-2505

3	Pelanggaran kepatuhan terkait privasi data dan regulasi TI	Audit internal berkala, pembatasan akses sesuai peran, penerapan kebijakan perlindungan data, serta verifikasi prosedur penyimpanan informasi.	Sedang	Sangat Besar	Tinggi
4	Gangguan infrastruktur TI (server, jaringan, *storage*)	*Monitoring* server otomatis, pemeliharaan berkala, *backup* data, serta redundansi jaringan untuk meminimalkan *downtime*.	Sedang	Besar	Sedang
5	Risiko akibat perubahan sistem atau implementasi teknologi baru	Pengujian *sandbox*, evaluasi teknis awal, uji integrasi, serta kontrol perubahan sebelum sistem dipindahkan ke lingkungan produksi.	Rendah	Besar	Rendah-Sedang
6	*Human error* dalam konfigurasi atau pengelolaan sistem	Prosedur operasional standar, pengecekan konfigurasi, dan verifikasi berlapis sebelum *deployment*.	Sedang	Sedang	Sedang

4.3 *Articulate Risk* (APO12.04)

Pada tahap ini, seluruh hasil identifikasi dan penilaian risiko disampaikan kepada manajemen agar dapat diprioritaskan dan diberikan tindakan pengendalian yang sesuai. Informasi mencakup peluang terjadinya risiko, urgensi risiko, serta rekomendasi tindak lanjut agar keputusan strategis dapat diambil dengan cepat dan terukur.

Berdasarkan hasil analisis risiko, rekomendasi yang diberikan difokuskan pada peningkatan pengendalian dan efektivitas pengelolaan risiko TI. Untuk risiko serangan siber, diperlukan penguatan sistem keamanan melalui peningkatan *firewall*, pemantauan *real-time*, dan autentikasi berlapis. Risiko *bug* aplikasi dapat diminimalkan dengan pengujian rutin, perbaikan proses quality assurance, serta mekanisme pelaporan *bug* yang lebih cepat.

Pada aspek kepatuhan, perusahaan perlu menyusun standar internal, melakukan audit berkala, serta meningkatkan kesadaran pegawai melalui pelatihan perlindungan data. Risiko infrastruktur dapat ditangani melalui pemeliharaan berkala, monitoring sistem, dan penyusunan rencana pemulihan layanan.

Sementara itu, risiko perubahan sistem perlu dikelola melalui analisis dampak, pengujian sebelum implementasi, serta dokumentasi yang baik. Adapun risiko human error dapat dikurangi melalui pelatihan teknis, penggunaan *checklist* operasional, serta penerapan proses review sebelum implementasi.

4.4 *Define A Risk Management Action Portfolio* (APO12.05)

Pada tahap ini, organisasi menetapkan langkah-langkah nyata untuk menangani setiap risiko TI yang telah diidentifikasi. Tujuannya adalah memastikan bahwa setiap risiko memiliki respons yang tepat, terukur, dan selaras dengan tingkat prioritasnya. Strategi respons risiko mencakup empat pendekatan utama:

1) *Avoid* (menghindari), mengubah proses atau sistem agar risiko tidak muncul.
2) *Mitigate* (mengurangi), menambah kontrol guna menurunkan peluang atau dampak.
3) *Transfer* (memindahkan), memindahkan sebagian risiko ke pihak ketiga, seperti vendor atau penyedia layanan.
4) *Accept* (menerima), menerima risiko yang dinilai kecil atau masih dalam batas toleransi organisasi.

p-ISSN : 2808-909X e-ISSN : 2798-2505

Strategi penanganan risiko pada PT. KLM didominasi oleh pendekatan mitigasi, dengan beberapa risiko tertentu juga menggunakan kombinasi strategi avoid, transfer, dan accept sesuai tingkat dampaknya. Risiko serangan siber ditangani melalui peningkatan proteksi keamanan, pemantauan jaringan, serta penyusunan SOP respons insiden oleh tim IT. Risiko bug aplikasi dikelola dengan pengujian rutin, perbaikan proses *quality assurance,* serta penerapan sistem pelacakan bug oleh tim developer dan IT.

Pada aspek kepatuhan, perusahaan menerapkan strategi *avoid* dan *mitigate* melalui penyusunan pedoman internal, audit berkala, serta pelatihan regulasi oleh manajemen dan tim IT. Risiko infrastruktur ditangani melalui pemeliharaan berkala, pembaruan perangkat, dan penyusunan rencana pemulihan oleh tim infrastruktur.

Sementara itu, risiko perubahan sistem dikelola dengan melibatkan vendor, memberikan pelatihan sebelum implementasi, serta menyusun dokumentasi perubahan oleh *project manager*. Adapun risiko human error ditangani melalui pelatihan teknis, penggunaan checklist operasional, serta penerapan proses review sebelum perubahan dilakukan oleh tim IT.

4.5 *Respond to Risk* (APO12.06)

Pada tahap APO12.06, organisasi memastikan bahwa seluruh risiko TI yang telah ditetapkan penanganannya dipantau secara terus menerus. Tujuannya adalah menilai apakah pengendalian berjalan efektif, apakah risiko berubah, dan apakah diperlukan penyesuaian rencana mitigasi.
Pemantauan dilakukan melalui:

a. evaluasi efektivitas kontrol,
b. peninjauan kembali tingkat risiko secara berkala,
c. pembaruan profil risiko apabila terjadi perubahan kondisi teknologi, proses, maupun lingkungan bisnis,
d. pelaporan rutin kepada manajemen mengenai status risiko, insiden yang terjadi, serta capaian mitigasi.

Melalui proses ini, organisasi dapat menjaga agar manajemen risiko tetap relevan dan selaras dengan kebutuhan operasional PT. KLM.

4.6 Tingkat Kapabilitas

Tahap analisis risiko dilakukan untuk mengetahui sejauh mana proses manajemen risiko TI pada PT. KLM telah berjalan sesuai dengan praktik yang direkomendasikan COBIT 5.0, khususnya pada domain APO12.01 hingga APO12.06. Untuk melakukan analisis ini, peneliti menggunakan instrumen berupa kuesioner yang disusun berdasarkan aktivitas utama pada setiap subproses APO12 Kuesioner dalam penelitian ini diisi oleh 2 responden yang merupakan *full-stack web developer* dan *mobile developer* di PT. KLM. Kuesioner disajikan dalam bentuk skala Likert 1–5, di mana responden diminta menilai tingkat kesesuaian pernyataan dengan kondisi aktual organisasi. Skala ini digunakan untuk mengukur objektivitas persepsi responden terhadap pelaksanaan kegiatan manajemen risiko TI. Adapun rentang penilaiannya adalah:
1 = Sangat Tidak Setuju
2 = Tidak Setuju
3 = Cukup Setuju
4 = Setuju
5 = Sangat Setuju

Penilaian diberikan untuk dua kondisi, yaitu:

a. *As-Is*, yang menggambarkan keadaan saat ini berdasarkan hasil wawancara dan observasi.
b. *To-Be*, yang merepresentasikan tingkat kapabilitas yang diharapkan organisasi untuk dicapai.

p-ISSN : 2808-909X e-ISSN : 2798-2505

Hasil pengisian kuesioner kemudian diolah dan dituangkan ke dalam tabel penilaian untuk melihat tingkat kesenjangan (*gap*) antara kondisi *As-Is* dan *To-Be*. Kesenjangan tersebut menjadi dasar dalam menentukan rekomendasi perbaikan proses manajemen risiko TI.

Berikut hasil penilaian *As-Is* dan *To-Be* pada masing-masing subproses APO12:

Tabel 4. Hasil Penilaian *As-Is* dan *To-Be*

Subproses	Rata-Rata *As-Is*	Rata-Rata *To-Be*	Level *As-Is*	Level *To-Be*
APO12.01 – Mengumpulkan Data	2.5	4.5	Level 2.5 (mendekati *Established*)	Level 4.5 (mendekati *Optimising*)
APO12.02 – Menganalisis Risiko	2.5	4.5	Level 2.5 (mendekati *Established*)	Level 4.5 (mendekati *Optimising*)
APO12.03 – Memelihara Profil Risiko	2.5	4.5	Level 2.5 (mendekati *Established*)	Level 4.5 (mendekati *Optimising*)
APO12.04 – Mengkomunikasikan Risiko	3.0	5.0	Level 3 (*Established*)	Level 5 (*Optimising*)
APO12.05 – Menentukan Tindakan Risiko	3.0	5.0	Level 3 (*Established*)	Level 5 (*Optimising*)
APO12.06 – Memantau Risiko	2.5	4.5	Level 2.5 (mendekati *Established*)	Level 2.5 (mendekati *Established*)

Rata-rata *As-Is* dan *To-Be* didapatkan dari penghitungan nilai dari masing-masing domain terdiri atas 2 butir pertanyan. Totalnya terdapat 12 pertanyaan yang telah dijawab responden.

Contoh penghitungannya adalah sebagai berikut:

a. Domain APO12.01

As-Is

$$NK = \frac{3+2}{2} = 2.5$$

To-Be

$$NK = \frac{5+4}{2} = 4.5$$

Berdasarkan rentang nilai:

b. Rata-rata *As-Is*
NK=(2.5+2.5+2.5+3.0+3.0+2.5) / 6 = 16/6 =2.67
Rata-rata nilai kapabilitas *As-Is* berada pada rentang Level 3, dengan subproses APO12.04 dan APO12.05 mencapai Level 3 penuh, sementara lainnya masih mendekati Level 2.51—3.0.

c. Rata-rata *To-Be*
NK=(4.5+4.5+4.5+5.0+5.0+4.5) / 6 = 28/6 =4.67
Masuk di rentang 4.51 – 5.00, sehingga levelnya 5 (*Optimising Process*)

Hasil penilaian menunjukkan bahwa tingkat kapabilitas manajemen risiko TI pada PT. KLM berada pada level 3 (*Established Process*). Artinya, sebagian besar aktivitas pengelolaan risiko telah berjalan dengan prosedur yang terdefinisi dan diterapkan secara konsisten, terutama dalam aspek pelaporan risiko dan penetapan respons risiko. Namun, beberapa subproses seperti pembaruan profil risiko, pengumpulan data

risiko, dan evaluasi efektivitas kontrol masih menunjukkan nilai yang stagnan pada level menengah, menandakan perlunya peningkatan mekanisme dokumentasi, monitoring, serta pemanfaatan sumber data yang lebih komprehensif.

Sementara itu, tingkat kapabilitas yang diharapkan (*To-Be*) ditargetkan berada pada level 5 (*Optimising Process*). Kondisi ini mencerminkan aspirasi organisasi untuk memiliki proses manajemen risiko TI yang tidak hanya stabil, tetapi juga adaptif, terukur, dan terus disempurnakan melalui evaluasi berkelanjutan. Kesenjangan antara *As-Is* dan *To-Be* sebesar dua tingkat menunjukkan perlunya perbaikan signifikan, khususnya pada integrasi data, automasi proses evaluasi, serta penjaminan bahwa setiap risiko dikelola berdasarkan praktik terbaik dan digunakan sebagai dasar dalam pengambilan keputusan strategis.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis manajemen risiko TI pada PT. KLM menggunakan domain APO12.01–APO12.06, dapat disimpulkan bahwa proses identifikasi, analisis, mitigasi, pemantauan, integrasi, serta evaluasi risiko telah berjalan, namun belum sepenuhnya terdokumentasi dan terintegrasi secara optimal. Hasil penilaian menunjukkan bahwa rata-rata tingkat kapabilitas pada kondisi *As-Is* berada pada Level 3 (*Established Process*), yang berarti proses telah terdefinisi dan dijalankan secara konsisten. Secara lebih rinci, subproses APO12.04 dan APO12.05 telah mencapai Level 3 secara penuh, sementara subproses lainnya masih berada pada rentang mendekati Level 3. Meskipun demikian, masih terdapat kesenjangan antara kondisi saat ini dengan target yang diharapkan, yaitu Level 5 (*Optimising Process*). Kesenjangan ini menunjukkan bahwa perusahaan masih perlu meningkatkan aspek dokumentasi formal, integrasi proses lintas unit, serta mekanisme pemantauan dan evaluasi yang lebih terstruktur dan berkelanjutan. Untuk meningkatkan efektivitas manajemen risiko TI, perusahaan disarankan menyusun dokumentasi formal pada setiap proses APO12, menetapkan matriks penilaian risiko yang baku, serta memastikan pemantauan dilakukan secara berkala melalui laporan tertulis kepada manajemen. Selain itu, perlu adanya kejelasan peran antar unit, penguatan kontrol preventif, serta penerapan evaluasi berbasis data agar pengelolaan risiko dapat berkembang secara adaptif dan berkelanjutan. Penelitian ini memiliki keterbatasan, yaitu penilaian kapabilitas masih didasarkan pada persepsi responden melalui kuesioner dan wawancara, sehingga belum sepenuhnya mencerminkan kondisi kinerja aktual secara kuantitatif. Selain itu, jumlah responden yang terbatas juga dapat memengaruhi tingkat generalisasi hasil penelitian.

DAFTAR PUSTAKA

[1] D. A. E. Saputri, A. Faroqi, and A. Wulansari, “Evaluation of Information Security Management Capability Level with COBIT 5,” *Bin. Digit. Technol.*, vol. 8, no. 1, pp. 726–737, 2025, doi: 10.32877/bt.v8i1.2682.

[2] E. Zuraidah, “Audit Tata Kelola Teknologi Informasi Management Menggunakan Framework Cobit 5 Pada Pt Simona,” *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 10, no. 1, pp. 1–6, 2023, doi: 10.30656/prosisko.v10i1.6099.

[3] ISACA, *A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL 60008 USA: ISACA, 2012.

[4] S. Farannisa, W. Agustika Nurtrisha, and D. Praditya, “Analisis Manajemen Risiko TI Menggunakan Kerangka Kerja COBIT 2019 Domain EDM03 dan APO12: Studi Kasus pada PT XYZ,” *Dhata Praditya Innov. J. Soc. Sci. Res.*, vol. 4, no. 4, pp. 11186–11199, 2024.

[5] R. Ardhyka, A. Fidaiyah, and R. Meiyanti, “Analisis Manajemen Risiko IT Menggunakan COBIT5 Pada Domain APO12,” *J. Inf. dan Teknol.*, vol. 5, no. 2, pp. 30–38, 2023, doi: 10.37034/jidt.v5i2.325.

[6] N. Butarbutar and A. R. Tanaamah, “Analisis Manajemen Risiko Menggunakan COBIT 5 Domain APO12 (Studi Kasus: Yayasan Bina Darma),” *J. Inf. Syst. Informatics*, vol. 3, no. 3, pp. 352–362, 2021, doi: 10.51519/journalisi.v3i3.155.

[7] A. L. Ayu, M. Lubis, L. Abdurrahman, I. F. Zamzami, R. A. Alqahtani, and R. Ramadhani, “Assessment of IT Risk Management at the Faculty of Industrial Engineering, Telkom University, Utilizing the COBIT 2019 Framework’s APO12 Domain with LAM INFOKOM Standards Mapping,” *Electron. Integr. Comput. Algorithm J.*, vol. 1, no. 2, pp. 50–56, 2024, doi:

p-ISSN : 2808-909X e-ISSN : 2798-2505

10.62123/enigma.v1i2.21.

[8] M. Meilinda, N. Julian Masidin, A. Dwitama, and S. Andayani, "Analisis Risk Management TI Menggunakan COBIT 5 Domain APO12 Pada Perusahaan XYZ Otomotif Di Palembang," *JuSiTik J. Sist. dan Teknol. Inf. Komun.*, vol. 8, no. 2, pp. 75–82, 2025, doi: 10.32524/jusitik.v8i2.1360.

[9] N. J. Budiono, A. D. Cahyono, and P. F. Tanaem, "Evaluasi Manajemen Risiko Teknologi Informasi Pada Perusahaan Daerah Air Minum Kota Salatiga Menggunakan Framework Cobit 5.0," *Sebatik*, vol. 25, no. 1, pp. 82–91, 2021, doi: 10.46984/sebatik.v25i1.1174.

[10] L. W. N. F. Fatimah and A. Ichwani, "Tata Kelola Teknologi Informasi Domain Apo12 Menggunakan Framework Cobit 5," *JIK J. Ilmu Komput.*, vol. 5, no. 1, pp. 31–41, 2020.