JURNAL TEKNIK INFORMATIKA DAN MULTIMEDIA Vol 6, No.1, Mei 2026, pp. 86 - 96
p-ISSN : 2808-909X (print)
e-ISSN : 2798-2505 (online)
http://journal.politeknik-pratama.ac.id/index.php/JTIM · page 86
DOI : https://doi.org/10.51903/informatika.v6i1.1512

ANALISIS RISIKO TI BPKP SUMSEL MENGGUNAKAN COBIT 5 DOMAIN APO12

Ayu Elisya Natama Sianturi[1*], Arron Mosses Jhon Hadi[2], Wianti Maharani[3], Sri Andayani[4]
[1, 2, 3, 4] Universitas Katolik Musi Charitas, Jalan Bangau No. 60, Ilir Timur II, Palembang, Sumatera Selatan
e-mail: [1]ayuelisyans@gmail.com, [2]arronmosses31@gmail.com, [3]maharaniwianti@gmail.com, [4]andayani_s@ukmc.ac.id.
[*] coresspondence

ARTICLE INFO

Article history:

Received 10 December 2026
Received in revised form 24 January 2026
Accepted 8 Mei 2026
Available online 15 Mei 2026

ABSTRACT

This study evaluates IT risk management at BPKP South Sumatra using the COBIT 5 APO12 domain. Findings show the current capability is at Level 3 (Established Process)—meaning processes are well-defined but need better monitoring and risk evaluation. To achieve proactive governance, the target is set at Level 5. The study concludes with a gap analysis and specific recommendations to bridge this performance jump.

***Keywords**: COBIT 5, APO12, IT Risk Management, Capability Level*

Abstrak

Penelitian ini bertujuan menilai tingkat kapabilitas proses manajemen risiko teknologi informasi pada BPKP Provinsi Sumatera Selatan menggunakan domain APO12 COBIT 5. Data diperoleh melalui wawancara dan penyebaran kuesioner yang mencakup aktivitas APO12.01–APO12.06. Hasil perhitungan menunjukkan bahwa kondisi *As-Is* berada pada Level 3 (*Established Process*), yang berarti proses telah berjalan dengan prosedur yang terdefinisi namun masih memerlukan peningkatan pada aspek *monitoring*, pelaporan mitigasi, dan evaluasi risiko. Sementara itu, kondisi *To-Be* ditetapkan pada Level 5 sebagai target untuk mewujudkan tata kelola TI yang lebih proaktif, efektif, dan berkelanjutan. Penelitian ini juga memberikan rekomendasi perbaikan berbasis analisis kesenjangan (*gap analysis*) antara kondisi saat ini dan kondisi yang diharapkan.
Kata Kunci: COBIT 5, APO12, manajemen risiko TI, tingkat kapabilitas.

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah membawa perubahan signifikan dalam tata kelola pemerintahan. Digitalisasi proses administrasi publik mendorong peningkatan efisiensi layanan dan transparansi, namun pada saat yang sama menimbulkan berbagai risiko baru yang dapat mempengaruhi keberlangsungan operasional serta keamanan data organisasi. Di sektor publik, risiko teknologi informasi tidak hanya mencakup gangguan sistem atau kebocoran data, tetapi juga berpotensi memengaruhi akuntabilitas dan integritas tata kelola pemerintahan. Oleh karena itu, penerapan manajemen risiko teknologi informasi menjadi elemen penting dalam mendukung tata kelola TI yang efektif dan berkelanjutan [1].

Dalam konteks kelembagaan pemerintah, Badan Pengawasan Keuangan dan Pembangunan (BPKP) memiliki mandat strategis untuk memastikan akuntabilitas pengelolaan keuangan negara serta pembangunan

Received December 10, 2025; Accepted Mei 8, 2026; Available online Mei 15, 2026

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

nasional. Peraturan Presiden Republik Indonesia Nomor 192 Tahun 2014 menetapkan bahwa BPKP bertugas menyelenggarakan pengawasan keuangan negara dan memberikan pembinaan terhadap Aparat Pengawasan Intern Pemerintah (APIP) di seluruh instansi [2]. Melalui peran tersebut, BPKP memanfaatkan berbagai aplikasi dan sistem informasi untuk mendukung proses audit, reviu, evaluasi, serta aktivitas pengawasan lainnya.

Implementasi sistem informasi dalam kegiatan audit dan *monitoring* internal terbukti meningkatkan efisiensi penyajian data serta mempercepat proses pengawasan. Namun, digitalisasi ini juga menghadirkan potensi risiko seperti serangan siber, gangguan sistem, kelemahan kontrol akses, dan kesalahan konfigurasi. Jika tidak dikelola dengan baik, risiko tersebut dapat menghambat efektivitas pengawasan dan menurunkan keandalan hasil pemeriksaan.

Untuk mengatasi tantangan tersebut, diperlukan penerapan manajemen risiko TI yang terstruktur dan mengacu pada standar yang diakui secara internasional. COBIT 5, yang dikembangkan oleh ISACA, menyediakan kerangka kerja komprehensif untuk tata kelola dan manajemen TI, termasuk domain APO12 (*Manage Risk*) yang secara khusus berfokus pada identifikasi, penilaian, mitigasi, dan pemantauan risiko TI [3]. Domain ini menekankan pentingnya pengelolaan risiko secara sistematis, terarah, dan terukur.

Berbagai penelitian sebelumnya menunjukkan bahwa domain APO12 pada COBIT 5 mampu membantu organisasi dalam membangun proses manajemen risiko TI yang lebih efektif. Studi-studi tersebut menemukan bahwa pendekatan APO12 memberikan gambaran objektif terhadap kapabilitas pengelolaan risiko, termasuk mengidentifikasi kebutuhan perbaikan pada organisasi yang masih berada pada tingkat kapabilitas dasar [4][5]. Penelitian lain juga menunjukkan bahwa proses manajemen risiko TI pada sejumlah instansi pemerintah masih belum konsisten dan terdokumentasi dengan baik, sehingga menghasilkan nilai kapabilitas yang relatif rendah [6]. Selain itu, pemanfaatan APO12 dalam lingkungan pemerintahan terbukti memperkuat upaya pemetaan risiko TI dan merumuskan langkah mitigasi yang lebih komprehensif [7]. Temuan terbaru bahkan menegaskan bahwa penerapan COBIT 5, khususnya domain APO12, membantu organisasi mengurangi potensi kerugian dan meningkatkan keandalan operasional melalui manajemen risiko TI yang lebih sistematis [4].

Kantor Perwakilan BPKP Provinsi Sumatera Selatan sebagai unit pelaksana pengawasan regional juga memanfaatkan sistem informasi untuk mendukung audit dan *monitoring*. Namun, dengan meningkatnya kompleksitas layanan digital dan ketergantungan pada infrastruktur TI, diperlukan evaluasi menyeluruh terhadap efektivitas manajemen risiko yang diterapkan. Oleh karena itu, penelitian ini bertujuan untuk menganalisis tingkat kapabilitas manajemen risiko TI pada Kantor Perwakilan BPKP Provinsi Sumatera Selatan menggunakan framework COBIT 5, khususnya domain APO12. Hasil penelitian ini diharapkan dapat memberikan rekomendasi strategis guna meningkatkan tata kelola risiko TI serta mendukung pengawasan berbasis teknologi yang andal dan berkelanjutan di lingkungan BPKP.

2. TINJAUAN PUSTAKA

2.1. *Teknologi Informasi dan Risiko TI*

Teknologi informasi telah menjadi pilar penting dalam transformasi pemerintahan modern, memungkinkan peningkatan efisiensi, transparansi, dan akses layanan publik. Namun, digitalisasi ini membawa konsekuensi risiko yang signifikan, seperti gangguan sistem, potensi kebocoran data, dan ancaman siber yang jika tidak diantisipasi dapat mengancam integritas dan keberlanjutan operasional organisasi publik [8][9]. Dalam konteks pemerintahan, pengelolaan risiko TI menjadi sangat krusial untuk menjaga keandalan sistem dan memastikan akuntabilitas dalam pelayanan publik.

2.2. *Manajemen Risiko Teknologi Informasi*

Manajemen risiko TI merupakan proses terstruktur yang mencakup identifikasi, analisis, evaluasi, tindakan mitigasi, dan pemantauan risiko untuk melindungi aset informasi dan mendukung tujuan organisasi. Standar seperti ISO 31000 menyajikan kerangka kerja formal untuk kegiatan ini, menekankan bahwa proses manajemen risiko harus sistematis, iteratif, dan berbasis konteks organisasi untuk menjadi efektif [10][11]. Dalam organisasi publik, pendekatan risiko TI harus melibatkan pemangku kepentingan untuk memastikan bahwa mitigasi risiko tidak hanya bersifat teknis tetapi juga selaras dengan kebijakan dan tujuan strategis.

2.3. *Framework COBIT 5*

COBIT 5 adalah kerangka kerja tata kelola dan manajemen TI yang banyak diadopsi oleh organisasi karena kemampuannya dalam menyelaraskan tujuan bisnis dengan praktik TI. *Framework* ini dirancang untuk memberikan panduan proses, *enabler*, serta prinsip yang membantu organisasi membangun struktur pengelolaan TI yang kuat dan terukur [12]. Dalam kerangka pemerintahan, COBIT 5 cocok digunakan karena menyediakan mekanisme untuk mengevaluasi bagaimana TI mendukung fungsi institusi publik sekaligus mengelola risiko secara strategis.

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

2.4. *Domain APO12 (Manage Risk)*

Domain APO12 pada COBIT 5 secara spesifik menangani pengelolaan risiko TI melalui rangkaian praktik yang mencakup pengumpulan data risiko, evaluasi profil risiko, penetapan tindakan mitigasi, serta pemantauan dan pelaporan risiko [13]. Praktik-praktik ini mencakup inventaris aset TI kritis, analisis probabilitas ancaman, komunikasi risiko kepada pemangku kepentingan, serta penentuan dan pengujian rencana respons risiko secara berkala. Dengan demikian, APO12 menjadi dasar penting bagi organisasi untuk memahami dan mengelola eksposur risiko TI secara proaktif.

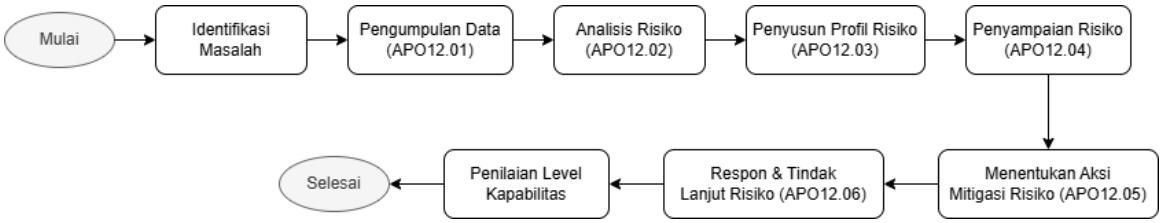
2.5. *Penelitian Terdahulu*

Berbagai penelitian telah menerapkan COBIT 5, khususnya domain APO12, untuk menilai kapabilitas manajemen risiko TI di institusi publik. Sebagai contoh, analisis pada Komisi Pemilihan Umum (KPU) menggunakan COBIT 5 menunjukkan bahwa proses manajemen risiko telah diterapkan tetapi belum terstruktur, dengan nilai kapabilitas rendah yang menunjukkan kebutuhan perbaikan dokumentasi dan kontrol [6]. Studi lain pada organisasi bisnis menggunakan COBIT 5 dan EDM03/APO12 juga menemukan gap antara kondisi aktual dan target kapabilitas, serta memberikan rekomendasi strategis untuk meningkatkan pengelolaan risiko [14].

3. METODOLOGI PENELITIAN

3.1. *Alur Penelitian*

Untuk memudahkan proses evaluasi manajemen risiko TI menggunakan COBIT 5 domain APO12, penelitian ini disusun dalam bentuk alur kerja yang sistematis. Setiap tahap dirancang untuk menggambarkan langkah-langkah mulai dari identifikasi masalah hingga penilaian kapabilitas proses, sehingga analisis dapat dilakukan secara terstruktur dan konsisten. Alur penelitian ini digambarkan melalui diagram alir (*flowchart*) berikut.



Gambar 1. *Flowchart* Alur Penelitian

3.2. *APO12.01 (Mengumpulkan Data)*

Tahap pertama dalam evaluasi domain APO12 adalah proses pengumpulan data risiko. Pada bagian ini, penelitian berfokus pada bagaimana instansi mengidentifikasi berbagai sumber risiko yang muncul dari aktivitas teknologi informasi. Informasi dikumpulkan melalui wawancara dengan pranata komputer dan auditor terampil. Hasil pengumpulan data ini menjadi fondasi penting untuk memahami pola risiko yang ada pada lingkungan TI BPKP Sumatera Selatan dan menjadi dasar bagi analisis risiko pada tahap selanjutnya.

3.3. *APO12.02 (Menganalisis Risiko)*

Setelah risiko teridentifikasi, penelitian memasuki tahapan analisis untuk menilai tingkat risiko berdasarkan aspek peluang terjadinya dan besarnya dampak yang dapat ditimbulkan. Setiap risiko dikaji sesuai dengan konteks operasional instansi. Proses analisis ini membantu menentukan prioritas penanganan risiko dan memetakan risiko mana yang memiliki urgensi tinggi, sedang, maupun rendah. Analisis yang dihasilkan kemudian menjadi rujukan bagi penyusunan profil risiko dan rekomendasi mitigasi.

3.4. *APO12.03 (Memelihara Profil Risiko)*

Tahap berikutnya adalah penyusunan dan pemeliharaan profil risiko. Pada bagian ini, risiko yang telah dianalisis dihimpun ke dalam sebuah dokumen yang memuat informasi lengkap seperti sumber risiko, penyebab, dampak, tingkat risiko, serta kontrol yang sudah tersedia. Profil risiko ini bukan hanya berfungsi sebagai dokumentasi, tetapi juga sebagai alat bantu manajemen dalam memahami kondisi risiko terkini dan memonitor perubahan risiko seiring berkembangnya sistem dan layanan TI. Dengan demikian, profil risiko menjadi dokumen yang bersifat dinamis dan harus diperbarui secara berkala.

3.5. *APO12.04 (Mengutarakan Risiko)*

Pada tahap ini, penelitian menilai bagaimana risiko yang telah dianalisis dikomunikasikan kepada pihak-pihak yang berkepentingan. Proses penyampaian risiko mencakup pelaporan hasil analisis, penjelasan tingkat prioritas, serta diskusi mengenai implikasi risiko terhadap layanan organisasi. Komunikasi risiko yang baik sangat penting agar manajemen dapat memahami situasi yang dihadapi dan merencanakan langkah-langkah yang diperlukan. Evaluasi ini juga melihat apakah proses penyampaian risiko dilakukan secara terstruktur dan diterima dengan baik oleh pengambil keputusan.

3.6. *APO12.05 (Menentukan Tindakan Manajemen Risiko)*

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

Pada tahap ini, fokus penelitian beralih pada bagaimana instansi menetapkan strategi penanganan risiko berdasarkan hasil analisis sebelumnya. Strategi mitigasi disesuaikan dengan tingkat risiko dan dapat berbentuk pengurangan risiko, pengalihan, penerimaan, ataupun penghindaran. Proses penentuan tindakan ini juga mempertimbangkan ketersediaan sumber daya, kebijakan internal, serta urgensi setiap risiko. Evaluasi dilakukan untuk memastikan bahwa tindakan yang direncanakan sudah relevan, terarah, dan mampu mengurangi eksposur risiko secara efektif.

3.7. *APO12.06 (Menanggapi Risiko)*

Tahap akhir dari evaluasi APO12 adalah penilaian terhadap bagaimana organisasi menindaklanjuti rencana mitigasi yang telah disusun. Pada bagian ini, penelitian mengkaji implementasi kontrol dan langkah penanganan risiko apakah telah dijalankan sesuai rencana, terdokumentasi, dan dievaluasi efektivitasnya. Respon risiko mencakup kegiatan *monitoring*, perbaikan berkelanjutan, serta pembaruan terhadap risiko residual yang masih tersisa. Evaluasi pada tahap ini menunjukkan sejauh mana organisasi mampu menerjemahkan rencana mitigasi ke dalam tindakan nyata yang berdampak pada penguatan pengelolaan risiko TI.

3.8. *Penilaian Risiko*

Proses penilaian risiko dilakukan berdasarkan nilai peluang dan dampak yang diberikan oleh responden dari BPKP Sumatera Selatan. Setiap risiko kemudian dihitung tingkatnya menggunakan matriks risiko agar dapat diketahui apakah risiko tersebut tergolong rendah, sedang, atau tinggi. Penilaian ini membantu organisasi memusatkan perhatian pada risiko yang paling kritis sekaligus memberikan gambaran objektif mengenai kondisi risiko TI yang dihadapi.

3.9. *Penilaian Tingkat Kapabilitas*

Penilaian kapabilitas dilakukan menggunakan model kapabilitas COBIT 5 yang terdiri dari enam level, mulai dari proses yang belum berjalan hingga proses yang telah dioptimalkan. Hasil penilaian kapabilitas diperoleh dengan mencocokkan hasil observasi dan bukti yang ditemukan pada setiap subproses APO12.01–APO12.06. Penilaian ini menghasilkan nilai kondisi aktual (*as-is*) yang kemudian dibandingkan dengan level target (*to-be*) yang ingin dicapai oleh organisasi. Perbandingan tersebut menjadi dasar untuk melakukan analisis kesenjangan dan merumuskan rekomendasi perbaikan. Berikut ini daftar level kapabilitas setiap subdomain APO12:

- Level 0 (*Non-Existent*): Rentang nilai 0 – 0,50 dengan nilai kapabilitas 0,00.
- Level 1 (*Performed Process*): Rentang nilai 0,51 – 1,50 dengan nilai kapabilitas 1,00.
- Level 2 (*Managed Process*): Rentang nilai 1,51 – 2,50 dengan nilai kapabilitas 2,00.
- Level 3 (*Established Process*): Rentang nilai 2,51 – 3,50 dengan nilai kapabilitas 3,00.
- Level 4 (*Predictable Process*): Rentang nilai 3,51 – 4,50 dengan nilai kapabilitas 4,00.
- Level 5 (*Optimising Process*): Rentang nilai 4,51 – 5,00 dengan nilai kapabilitas 5,00.

Hasil perhitungan level kapabilitas digunakan untuk menentukan level kapabilitas baik pada kondisi saat ini (*As-Is*) maupun kondisi yang diharapkan (*To-Be*). Rumus perhitungan nilai kapabilitas ditunjukkan sebagai berikut: $NK = \frac{\sum(Skor_Pertanyaan)}{Jumlah_Pertanyaan}$

4. HASIL DAN PEMBAHASAN

4.1 *APO12.01 Mengumpulkan Data*

Tahap pengumpulan data risiko dilakukan melalui wawancara dengan Pranata Komputer dan Auditor Terampil di BPKP Provinsi Sumatera Selatan, serta melalui peninjauan dokumen internal dan observasi lapangan. Dari proses tersebut, teridentifikasi delapan risiko utama yang berkaitan dengan aspek keamanan, integrasi data, kesalahan pengguna, infrastruktur, hingga keterbatasan sumber daya. Risiko-risiko ini menunjukkan bahwa meskipun operasional TI telah berjalan dengan dukungan pusat, masih terdapat kerentanan yang perlu diperhatikan untuk memastikan keberlanjutan dan keandalan layanan teknologi informasi di lingkungan BPKP Sumsel. Rincian risiko yang teridentifikasi ditampilkan pada Tabel 1 berikut.

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

Tabel 1. Identifikasi Risiko

No.	Kategori Risiko	Deskripsi Risiko	Dampak Potensial
1.	Keamanan Sistem dan Data	Potensi serangan siber dan kebocoran data akibat aplikasi yang belum sepenuhnya terintegrasi.	Gangguan layanan, kebocoran data, dan menurunnya kepercayaan publik.
2.	Redundansi & Integrasi Data	Duplikasi data dan lambatnya sinkronisasi antar aplikasi akibat keterbatasan integrasi antarinstansi.	Inkonsistensi data, keterlambatan pelaporan, dan kesalahan analisis.
3.	*Human Error*	Kesalahan input serta ketidaksiapan user saat terjadi perubahan aplikasi.	Informasi tidak akurat, gangguan proses kerja, dan penurunan efisiensi.
4.	Kegagalan Sistem/Perangkat	Risiko kerusakan perangkat atau gangguan jaringan lokal meski dipantau pusat.	*Downtime* sistem yang menyebabkan terganggunya operasional.
5.	Pemadaman Listrik & Infrastruktur	Potensi gangguan daya pada server lokal meski tersedia UPS dan genset.	Terhentinya layanan yang menyebabkan kemungkinan kehilangan data.
6.	Pelaporan Insiden Tidak Optimal	Pegawai belum seluruhnya mengetahui kanal pelaporan resmi Aplikasi Polite/*Helpdesk* IT.	Penanganan insiden terlambat dan risiko berulang tidak tercatat.
7.	Keterbatasan SDM TI	Ketergantungan tinggi pada pusat dan vendor untuk penanganan teknis.	Keterlambatan pemeliharaan dan mitigasi risiko kurang optimal.
8.	*Update* Aplikasi Terlambat Disosialisasikan	Pembaruan aplikasi tidak langsung diinformasikan ke *user*.	Produktivitas menurun dan potensi kesalahan operasional meningkat.

4.2 *APO12.02 Menganalisis Risiko*

Setelah seluruh risiko diidentifikasi, tahap berikutnya adalah melakukan analisis untuk menilai tingkat peluang terjadinya risiko, besarnya dampak yang ditimbulkan, serta efektivitas pengendalian yang tersedia. Proses analisis ini dilakukan dengan mempertimbangkan kondisi operasional di BPKP Sumatera Selatan, mekanisme kerja tiap aplikasi, serta kesiapan infrastruktur dan sumber daya manusia. Hasil analisis menunjukkan bahwa sebagian besar risiko memiliki dampak sedang hingga tinggi, terutama yang terkait dengan keamanan data, integrasi sistem, dan kesalahan pengguna. Meski demikian, peluang terjadinya risiko dapat ditekan melalui penguatan kontrol yang sudah berjalan dan peningkatan koordinasi antarunit. Rangkuman analisis risiko ditampilkan pada Tabel 2 berikut.

Tabel 2. Analisis Risiko

No.	Risiko	Pengendalian	Peluang	Dampak
1.	Serangan siber terhadap sistem aplikasi	*Firewall*, enkripsi, autentikasi berlapis, monitoring, backup otomatis, kebijakan keamanan, dan rencana tanggap insiden	Sedang	Sangat Besar
2.	Redundansi dan integrasi data	Integrasi data lintas lini dan antarinstansi	Sedang	Besar
3.	*Human error*	Pelatihan berkala, SOP, dan pembatasan akses sesuai otoritas	Besar	Sedang
4.	Kegagalan sistem/perangkat keras	Peremajaan infrastruktur dan pemeliharaan rutin	Sedang	Besar
5.	Pemadaman listrik	Penggunaan UPS dan genset untuk menjaga keberlangsungan server	Kecil	Sedang
6.	Kurangnya sosialisasi pelaporan insiden	Kanal resmi (Polite & IT *Helpdesk* WA) dan sosialisasi kepada pegawai	Sedang	Sedang
7.	Keterbatasan SDM TI	Pelatihan teknis, koordinasi dengan pusat, dukungan vendor, dan dokumentasi dan SOP	Besar	Besar
8.	Keterlambatan *update* aplikasi	Jadwal pembaruan rutin, notifikasi otomatis, koordinasi pengembang–*user*, dan panduan perubahan aplikasi	Sedang	Sedang

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

4.3 *APO12.03 Memelihara Profil Risiko*

Setelah risiko dianalisis, langkah berikutnya adalah menyusun dan memelihara profil risiko sebagai dokumentasi resmi manajemen risiko TI. Profil risiko ini disusun berdasarkan tingkat peluang dan dampak yang diperoleh dari tahapan sebelumnya, sehingga menghasilkan pemetaan tingkat risiko yang dapat menjadi dasar penentuan prioritas mitigasi. Pada tahap ini, seluruh risiko yang telah teridentifikasi dikelompokkan menurut tingkat keparahannya dan disimpan sebagai bagian dari dokumen pengelolaan risiko yang digunakan oleh BPKP Sumatera Selatan. Pemeliharaan profil ini bertujuan untuk memastikan bahwa setiap risiko tercatat, terpantau, serta dapat diperbarui secara berkala sesuai dinamika operasional TI. Rincian tingkat risiko ditampilkan pada Tabel 3 berikut.

Tabel 3. Profil Risiko

No.	Risiko	Tingkat Risiko
1.	Serangan siber terhadap sistem aplikasi	Sangat Besar
2.	Redundansi dan integrasi data	Besar
3.	*Human error*	Sedang
4.	Kegagalan sistem atau perangkat keras	Besar
5.	Pemadaman listrik	Sedang
6.	Kurangnya sosialisasi pelaporan insiden	Sedang
7.	Keterbatasan SDM TI di perwakilan	Besar
8.	Keterlambatan *update* aplikasi	Sedang

4.4 *APO12.04 Mengutarakan Risiko*

Hasil identifikasi dan analisis yang telah dilakukan sebelumnya disusun menjadi informasi yang mudah dipahami oleh manajemen. Proses ini memastikan bahwa setiap risiko beserta peluang terjadinya dan rekomendasi pengendaliannya disajikan secara jelas sehingga mendukung pengambilan keputusan yang tepat. Penyampaian risiko dilakukan melalui penyusunan laporan risiko yang menyoroti prioritas risiko utama, seperti ancaman siber, keterbatasan sumber daya manusia TI, serta keterlambatan pembaruan aplikasi. Informasi tersebut menjadi dasar penentuan langkah mitigasi yang perlu ditindaklanjuti secara terencana. Rincian penyampaian risiko ditunjukkan pada Tabel 4 berikut.

Tabel 4. Pengendalian Risiko

No.	Risiko	Peluang	Rekomendasi
1.	Serangan siber terhadap sistem aplikasi	Sedang	Perkuat *firewall*, enkripsi, MFA, *monitoring*, audit keamanan, dan bentuk CSIRT tingkat perwakilan yang terhubung ke pusat.
2.	Redundansi dan integrasi data	Sedang	Percepat integrasi antarunit, bangun *data warehouse* terpusat, tetapkan standar pertukaran data (API & format baku), serta perbarui MoU kerja sama data.
3.	*Human error*	Besar	Lakukan pelatihan rutin, terapkan validasi *input* otomatis, dan perjelas tanggung jawab pengguna melalui SOP dan evaluasi kinerja.
4.	Kegagalan sistem atau perangkat keras	Sedang	Lakukan peremajaan perangkat, *monitoring real-time*, serta uji dan perbarui *Disaster Recovery Plan* minimal dua kali setahun.
5.	Pemadaman listrik	Kecil	Pastikan genset dan UPS dalam kondisi prima, lakukan pengujian beban berkala, dan pertimbangkan pemindahan penyimpanan ke *cloud*/pusat data nasional.
6.	Kurangnya sosialisasi pelaporan insiden	Sedang	Lakukan sosialisasi melalui *banner*, *email*, dan sesi internal; gunakan sistem tiket insiden agar pelaporan terdokumentasi dan dapat dipantau.
7.	Keterbatasan SDM TI	Besar	Tingkatkan pelatihan teknis, perkuat koordinasi dengan pusat, manfaatkan vendor/*outsourcing*, dan jalankan SOP untuk menjaga keberlanjutan layanan.

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

8.	Keterlambatan *update* aplikasi	Sedang	Tetapkan jadwal *update*, gunakan notifikasi otomatis, lakukan uji coba sebelum implementasi, dan jaga komunikasi resmi antara pengembang dan pengguna.

4.5 *APO12.05 Menentukan Tindak Manajemen Risiko*

Tahap penentuan tindakan manajemen risiko dilakukan untuk memastikan bahwa setiap risiko TI yang telah diidentifikasi, dianalisis, dan diprioritaskan memperoleh penanganan yang sesuai. Pada BPKP Provinsi Sumatera Selatan, proses ini mencakup pemilihan strategi respons risiko yang paling relevan dengan kondisi organisasi. Strategi ini dapat berupa penghindaran (*avoid*), pengurangan (*mitigate*), pemindahan (*transfer*), ataupun penerimaan (*accept*), bergantung pada tingkat dampak dan peluang risiko.

Setelah strategi ditetapkan, organisasi menyusun rencana tindak lanjut berupa *risk treatment plan* yang menjelaskan langkah-langkah operasional, penanggung jawab, serta sumber daya yang diperlukan. Rencana tersebut disusun untuk memastikan setiap risiko mendapatkan intervensi yang proporsional dengan urgensinya. Tabel 5 berikut merangkum strategi dan tindakan penanganan risiko yang direncanakan berdasarkan hasil analisis sebelumnya.

Tabel 5. Tindak Manajemen Risiko

Risiko	Strategi Penanganan	Tindakan yang Direncanakan	Penanggung Jawab
Serangan siber terhadap sistem aplikasi	*Mitigate*	Peningkatan *firewall*, enkripsi, MFA, dan audit keamanan berkala	Tim TI & BPKP Pusat
Redundansi dan integrasi data	*Mitigate*	Pengembangan integrasi antarunit, standar pertukaran data, sinkronisasi terjadwal	Tim TI & Koordinator SPBE
Human error	*Mitigate*	Pelatihan rutin, validasi *input* otomatis, peninjauan SOP pengguna	Subbag Umum & Kepegawaian
Kegagalan sistem/perangkat keras	*Mitigate*	Pemeliharaan perangkat rutin, *monitoring* infrastruktur, penyusunan DRP	Pranata Komputer & Tim Infrastruktur
Pemadaman listrik	*Mitigate*	Pemanfaatan UPS/genset, uji beban rutin, replikasi data ke *cloud*	Tim Sarana Prasarana & TI
Kurangnya sosialisasi pelaporan insiden	*Mitigate*	Sosialisasi kanal pelaporan, penggunaan sistem tiket insiden, *monitoring* laporan	Tim TI & Humas
Keterbatasan SDM TI di perwakilan	Transfer & *Mitigate*	Pelatihan teknis, koordinasi dengan pusat, kolaborasi vendor eksternal	Kepala Perwakilan & Tim TI
Keterlambatan *update* aplikasi	*Mitigate*	Jadwal update terencana, uji coba versi, notifikasi perubahan ke pengguna	Tim TI & Pengembang Aplikasi

4.6 *APO12.06 Menanggapi Risiko*

Tahap ini berfokus pada kegiatan pemantauan dan peninjauan berkelanjutan untuk memastikan bahwa seluruh tindakan mitigasi risiko telah berjalan sesuai rencana serta tetap relevan dengan dinamika operasional organisasi. Di BPKP Provinsi Sumatera Selatan, proses penanganan risiko tidak dilakukan secara mandiri, karena sebagian besar pengelolaan risiko TI berada di bawah kewenangan BPKP Pusat. Perwakilan hanya menjalankan tindak lanjut berdasarkan arahan pusat dan hasil audit TI yang dilakukan sekitar dua kali dalam setahun, di mana penilaian risiko dilakukan menggunakan COBIT 5.

Kondisi tersebut menunjukkan bahwa proses penanganan dan pemantauan risiko di tingkat perwakilan belum dilakukan secara proaktif dan berkelanjutan, melainkan masih bergantung pada arahan dari BPKP Pusat. Hal ini mengindikasikan bahwa kapabilitas pada subdomain APO12.06 masih berada pada tingkat yang belum optimal, khususnya dalam aspek monitoring dan evaluasi risiko secara mandiri.

Secara praktis, kondisi ini dapat berdampak pada keterlambatan dalam mengidentifikasi perubahan risiko serta kurang optimalnya evaluasi terhadap efektivitas tindakan mitigasi yang telah diterapkan. Selain itu, ketergantungan pada pusat juga berpotensi menghambat respons cepat terhadap risiko yang bersifat lokal dan spesifik di tingkat perwakilan. Oleh karena itu, diperlukan penguatan mekanisme monitoring risiko

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

secara lebih mandiri dan berkala agar organisasi mampu meningkatkan kapabilitas pengelolaan risiko secara menyeluruh.

4.7 *Tingkat Kapabilitas*

4.7.1 *Instrumen Penilaian (Kuesioner)*

Penilaian tingkat kapabilitas dilakukan menggunakan kuesioner yang disusun berdasarkan aktivitas APO12.01 hingga APO12.06. Setiap pertanyaan mewakili praktik yang seharusnya diterapkan dalam proses manajemen risiko menurut COBIT 5. Responden memberikan skor pada skala 0–5 untuk menggambarkan tingkat penerapan saat ini. Instrumen ini digunakan untuk menilai kondisi *As-Is* dan membandingkannya dengan target *To-Be* sebagaimana yang diharapkan oleh organisasi.

Kuesioner disusun terstruktur berdasarkan aktivitas pada domain COBIT 5 APO12. Instrumen ini dirancang untuk mengevaluasi manajemen risiko TI melalui beberapa tahapan kunci. Pertama, pada tahap pengumpulan data (APO12.01), dievaluasi sejauh mana organisasi mengidentifikasi risiko secara sistematis dan mendokumentasikannya ke dalam *risk register*. Selanjutnya, aspek analisis risiko (APO12.02) meninjau ketegasan manajemen dalam menetapkan serta mengomunikasikan batas toleransi risiko kepada unit terkait.

Tahap berikutnya fokus pada pemeliharaan profil risiko (APO12.03) yang mencakup penggunaan parameter dampak dan kemungkinan dalam penentuan prioritas, serta penyampaian risiko (APO12.04) yang menilai kualitas laporan formal kepada manajemen. Terakhir, kuesioner ini mengukur efektivitas dalam menentukan tindakan mitigasi (APO12.05) yang harus memiliki penanggung jawab dan sumber daya yang jelas, serta proses menanggapi risiko (APO12.06) melalui pemantauan status risiko secara berkala dan peninjauan risiko baru demi perbaikan tata kelola yang berkelanjutan.

4.7.2 *Hasil Penilaian (As-Is dan To-Be)*

Penilaian dilakukan menggunakan sejumlah pertanyaan kuesioner yang berfungsi untuk mengetahui kondisi penerapan proses manajemen risiko saat ini (*As-Is*) serta target yang ingin dicapai (*To-Be*). Setiap pertanyaan dijawab oleh responden dengan jabatan Pranata Komputer di BPKP Pusat yang memahami proses pengelolaan TI di BPKP Pusat. Pemilihan responden dari BPKP Pusat didasarkan pada fakta bahwa pengelolaan risiko TI di seluruh perwakilan mengikuti kebijakan, standar, dan arahan yang ditetapkan secara terpusat. Dengan demikian, penilaian yang diberikan oleh responden dianggap mewakili kondisi yang berlaku secara umum, termasuk pada BPKP Provinsi Sumatera Selatan. Hasil penilaian tersebut kemudian dituangkan dalam bentuk tabel *As-Is* dan *To-Be* sebagaimana ditunjukkan pada Tabel 6.

Tabel 6. Tabel *As-Is* dan *To-Be*

No	Aktivitas	As-Is	To-Be	Gap
APO12.01	**Mengumpulkan Data**	**3.3**	**5**	**1.7**
1	Identifikasi risiko TI dilakukan secara sistematis	3	5	2
2	Identifikasi risiko dilakukan secara berkala	3	5	2
3	Hasil identifikasi terdokumentasi dalam *risk register*	4	5	1
APO12.02	**Menganalisis Risiko**	**4.3**	**5**	**0.7**
4	Manajemen menetapkan batas toleransi risiko	5	5	0
5	Toleransi risiko dikomunikasikan kepada unit terkait	4	5	1
6	Keputusan menerima/menolak risiko mengikuti toleransi	4	5	1
APO12.03	**Memelihara Profil Risiko**	**3.3**	**5**	**1.7**
7	Risiko dianalisis menggunakan dampak & kemungkinan	4	5	1
8	Organisasi memiliki matriks risiko	4	5	1
9	Analisis risiko diperbarui ketika ada perubahan sistem	2	5	3

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

APO12.04	**Mengutarakan Risiko**	**3.3**	**5**	**1.7**
10	Hasil evaluasi risiko dilaporkan secara formal	2	5	3
11	Laporan risiko berisi deskripsi, tingkat risiko, rekomendasi	4	5	1
12	Komunikasi risiko dilakukan secara jelas	4	5	1
APO12.05	**Menentukan Tindakan Mitigasi**	**3.3**	**5**	**1.7**
13	Tindakan mitigasi ditetapkan untuk seluruh risiko TI	3	5	2
14	Mitigasi memiliki penanggung jawab, waktu & resource	4	5	1
15	Efektivitas mitigasi dievaluasi	3	5	2
APO12.06	**Menanggapi Risiko**	**2.3**	**5**	**2.7**
16	Status risiko dimonitor secara berkala	2	5	3
17	Perkembangan mitigasi dilaporkan secara rutin	2	5	3
18	Risiko baru diidentifikasi dan ditinjau	3	5	2
RATA-RATA	**TOTAL KAPABILITAS**	**3.3**	**5**	**1.7**

4.7.3 *Penilaian Level Kapabilitas*

Penilaian level kapabilitas dilakukan untuk mengetahui sejauh mana proses APO12 telah diterapkan pada BPKP Provinsi Sumatera Selatan. Pengukuran dilakukan berdasarkan skor kuesioner yang diberikan responden terhadap setiap sub-proses APO12. Skor yang diperoleh kemudian dihitung menggunakan rumus nilai kapabilitas COBIT 5. Hasil akhirnya dibandingkan dengan rentang nilai *capability level*, sehingga dapat ditentukan tingkat kapabilitas *As-Is* dan target *To-Be* yang diharapkan.

Sebagai contoh, perhitungan pada sub-proses APO12.01 (Mengumpulkan Data) menunjukkan bahwa tiga pertanyaan memperoleh skor 3, 3, dan 4. Dengan demikian:

$$NK = \frac{3+3+4}{3} = \frac{10}{3} = 3.33$$

Nilai tersebut termasuk dalam rentang 2.51–3.50, sehingga APO12.01 berada pada Level 3 (*Established Process*). Sementara untuk kondisi *To-Be*, seluruh skor ditetapkan pada level maksimal (5), sehingga nilai kapabilitas menjadi 5.00 atau Level 5 (*Optimising Process*).

Rekapitulasi nilai kapabilitas seluruh sub-proses APO12 ditampilkan pada Tabel 7 berikut.

Tabel 7. Rekapitulasi Nilai

No.	Subdomain APO12	Nilai Kapabilitas As-Is	Nilai Kapabilitas To-Be	Level As-Is	Level To-Be
1.	APO12.01 (Mengumpulkan Data)	3.33	5.00	3	5
2.	APO12.02 (Menganalisis Risiko)	4.33	5.00	4	5
3.	APO12.03 (Memelihara Profil Risiko)	3.33	5.00	3	5
4.	APO12.04 (Mengutarakan Risiko)	3.33	5.00	3	5
5.	APO12.05 (Menentukan Tindakan Mitigasi)	3.33	5.00	3	5
6.	APO12.06 (Menanggapi Risiko)	2.33	5.00	2	5
Rata-rata		**3.16**	**5.00**	**3**	**5**

Berdasarkan hasil tersebut, rata-rata nilai kapabilitas *As-Is* berada pada Level 3 (*Established Process*), menunjukkan bahwa proses manajemen risiko TI telah diterapkan secara konsisten dan didukung prosedur yang terdokumentasi. Namun, proses belum mencapai tahap yang sepenuhnya terukur atau proaktif. Target *To-Be* ditetapkan pada Level 5 (*Optimising Process*), yang menggambarkan aspirasi organisasi untuk meningkatkan proses secara berkelanjutan, adaptif, dan terintegrasi sesuai standar COBIT 5.

5. KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa tingkat kapabilitas manajemen risiko TI pada BPKP Provinsi Sumatera Selatan, berdasarkan domain APO12 COBIT 5, berada pada Level 3.16 yang mengonfirmasi posisi pada level 3 (*Established Process*). Artinya, proses sudah terdokumentasi dan dijalankan secara konsisten, tetapi belum mencapai tingkat yang sepenuhnya terukur atau proaktif. Analisis menunjukkan bahwa pengelolaan risiko TI telah berjalan cukup baik pada beberapa aspek, namun masih terdapat kelemahan pada pemantauan risiko, pelaporan perkembangan mitigasi, serta evaluasi efektivitas tindakan mitigasi. Kesenjangan antara kondisi *As-Is* dan praktik ideal COBIT 5 terutama terlihat pada belum tersedianya mekanisme monitoring risiko yang berkelanjutan.

Sebagai saran, BPKP Sumsel perlu memperkuat proses pemantauan risiko secara lebih rutin, memperbaiki kualitas dan konsistensi pelaporan, serta memastikan penanggung jawab mitigasi ditetapkan secara jelas. Pembaruan *risk register* saat terjadi perubahan sistem, penggunaan format laporan yang lebih baku, dan peningkatan kompetensi SDM dalam manajemen risiko TI juga menjadi langkah penting untuk menutup *gap* yang ada. Dengan perbaikan tersebut, organisasi diharapkan mampu meningkatkan kapabilitas pengelolaan risiko TI menuju level yang lebih tinggi serta mendukung tata kelola TI yang lebih efektif dan berkelanjutan.

DAFTAR PUSTAKA

[1] E. Yulisuyanti and S. Benfano, "Model Manajemen Risiko Sistem Informasi Untuk Sistem Informasi Manajemen Kepegawaian," *Techno.COM*, vol. 22, no. 3, pp. 783–795, 2023.

[2] bpkp.go.id, "Profil BPKP," bpkp.go.id. Accessed: Nov. 16, 2025. [Online]. Available: https://www.bpkp.go.id/id/tentang/profil

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

[4] M. Maharani, A. Klasmanto, B. A. Simanjuntak, and S. Andayani, "IT-EXPLORE Manajemen risiko teknologi informasi pada PT . XYZ menggunakan framework COBIT 5," *J. Penerapan Teknol. Inf. dan Komun.*, vol. 04, no. 02, pp. 173–185, 2025, doi: 10.24246/itexplore.v4i2.2025.pp173-185.

[5] J. S. A. Rajjani, B. T. Hanggara, and Y. T. Musityo, "Evaluasi Manajemen Risiko Teknologi Informasi pada Department of ICT PT Semen Indonesia (Perseo) Tbk menggunakan Framework COBIT 2019 dengan Domain EDM03 dan APO12," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 5, pp. 1734–1744, 2021.

[6] M. A. Wirayudha, "Analysis of Information Technology Risk Management at KPU Using Cobit 5 Domain APO12 Analisis Manajemen Risiko Teknologi Informasi pada KPU Menggunakan Cobit 5 Domain APO12," *MALCOM Indones. J. Mach. Learn. Comput. Sci. J.*, vol. 4, no. April, pp. 433–442, 2024.

[7] H. Ani, N. Sari, Y. Rahardja, and H. P. Chernovita, "Analisis Manajemen Risiko TI Pada Diskominfo Salatiga Menggunakan Cobit5 Dengan Domain Apo12," *J. Tek. Inform. dan Sist. Inf.*, vol. 8, no. 4, pp. 1772–1784, 2021.

[8] L. Febriyanti, M. Febrinazahra, Kraugusteeliana, and I. G. S. Masdiyasa, "Manajemen Risiko Sistem Informasi Unit Organisasi Bpiw Kementerian Pupr Menggunakan Framework Iso 31000:2018," *J. Sist. Inf. dan Apl.*, vol. 2, no. 2, pp. 1–12, 2024, [Online]. Available: https://ejournal.upnvj.ac.id/jsia/article/view/5907

[9] A. Kurniati, L. Edi Nugroho, and M. Nur Rizal, "Information Technology Risk Management on e-Government: Systematic Literature Review," *J. Ilmu Pengetah. dan Teknol. Komun.*, vol. 22, no. 2, pp. 207–222, 2020, [Online]. Available: http://dx.doi.org/10.33164/iptekkom.22.2.2020.207-222

[10] N. S. H, "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 (Studi Kasus: Sistem Infrastruktur TI Telkom Indonesia)," *J. Sains, Teknol. dan Ind.*, vol. 9, no. 1, pp. 52–66, 2011, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/sitekin/article/view/607

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

[11] R. A. Zulfikri, D. Yuniarto, and D. Setiadi, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000 berkembang yang berdampak pada segala aspek kehidupan manusia . Semua termasuk Aplikasi Kehadiran Mobile (K-Mob) merupakan salah satu penerapan dari pengguna teknologi informa," *SABER J. Tek. Inform. Sains, dan Ilmu Komun.*, vol. 3, no. 3, pp. 350–362, 2025.

[12] F. Greene, "Selected COBIT 5 Processes for Essential Enterprise Security," *Isaca J.*, vol. 2, pp. 1–3, 2015.

[13] S. Salman, "COBIT 5 for Risk: Making Sense of IT Risk Management," isaca.org. Accessed: Nov. 21, 2025. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2017/cobit-5-for-risk-making-sense-of-it-risk-management

[14] A. Purwanto and I. Riadi, "Analysis of Risk Management Assessment on Quality Control Services using Framework COBIT 5," *Int. J. Comput. Appl.*, vol. 183, no. 29, pp. 17–25, 2021.