

Manajemen Risiko TI Pada BID TIK Polda Sumsel Menggunakan Framework Cobit 5

Mutia Maharani^{1*}, Andri Wijaya²

¹⁻²Sistem Informasi, Universitas Katolik Musi Charitas Palembang

¹⁻²Jl. Bangau No. 60, Kec. Ilir Timur III Palembang

Email: mutiamhrni29@gmail.com¹, andri_wijaya@ukmc.ac.id²

Abstract

Information technology plays a key role in supporting operational effectiveness, including in government institutions such as the Indonesian National Police. BID TIK POLDA SUMSEL is responsible for managing information and communication technology systems, supported by three subdivisions: Renmin, Tekkom, and Tekinfo. Various IT risks such as human error, network disruptions, hardware failures, and undocumented incidents have been identified. To manage these risks effectively, a structured approach using COBIT 5—particularly the APO12 (Manage Risk) domain—was applied. This domain provides systematic guidance in identifying, assessing, and mitigating IT risks. The study analyzed six APO12 subprocesses through questionnaires and capability level scoring. The current (As Is) average score was 2.07 (Level 2), showing processes are executed but not consistently documented. The desired (To Be) score was 3.43 (Level 3), indicating a goal of standardized and documented processes. The identified gap highlights the need for improved documentation, coordination, and use of technology in IT risk management.

Key Words: APO12, COBIT 5, Information Technology, Risk Management, South Sumatra Regional Police

Abstrak

Teknologi informasi memegang peranan penting dalam mendukung efektivitas operasional, termasuk di institusi pemerintah seperti Kepolisian Republik Indonesia. BID TIK POLDA SUMSEL bertanggung jawab dalam mengelola sistem teknologi informasi dan komunikasi, yang didukung oleh tiga subbidang: Renmin, Tekkom, dan Tekinfo. Berbagai risiko TI seperti kesalahan manusia, gangguan jaringan, kegagalan perangkat keras, dan insiden yang tidak terdokumentasi telah diidentifikasi. Untuk mengelola risiko-risiko tersebut secara efektif, pendekatan terstruktur menggunakan COBIT 5-khususnya domain APO12 (Manage Risk)-diterapkan. Domain ini memberikan panduan sistematis dalam mengidentifikasi, menilai, dan memitigasi risiko TI. Penelitian ini menganalisis enam subproses APO12 melalui kuesioner dan penilaian tingkat kapabilitas. Skor rata-rata saat ini (As Is) adalah 2,07 (Level 2), yang menunjukkan bahwa proses-proses dijalankan tetapi tidak didokumentasikan secara konsisten. Skor yang diinginkan (To Be) adalah 3,43 (Level 3), yang menunjukkan tujuan proses yang terstandardisasi dan terdokumentasi. Kesenjangan yang teridentifikasi menyoroti perlunya peningkatan dokumentasi, koordinasi, dan penggunaan teknologi dalam manajemen risiko TI.

Kata Kunci: APO12, COBIT 5, Manajemen Risiko, Polisi Daerah Sumatera Selatan, Teknologi Informasi.

Pendahuluan

Teknologi informasi menjadi elemen penting dalam mendukung operasional organisasi dalam mencapai efisiensi dan efektivitas kerja [1]. Tidak hanya di sektor bisnis peran teknologi informasi juga dimanfaatkan oleh institusi pemerintahan khususnya Kepolisian Republik Indonesia, dalam menyediakan layanan teknologi informasi dan komunikasi yang mendukung tugas kepolisian dalam pelayanan dan keamanan untuk masyarakat. Salah satu bagian yang memiliki peran penting dalam pengelolaan dan pengembangan teknologi informasi di lingkungan kepolisian adalah BID TIK POLDA SUMSEL.

BID TIK POLDA SUMSEL (Bidang Teknologi Informasi dan Komunikasi Polisi Daerah Sumatera Selatan) merupakan organisasi khusus menangani masalah teknologi informasi yang bertugas dalam

pembinaan teknologi informasi dan komunikasi, pengumpulan dan pengolahan data, serta penyajian informasi keamanan dan ketertiban masyarakat (Kamtibmas) dan pelayanan multimedia [2]. Untuk mendukung pelaksanaan tugas tersebut, BID TIK POLDA SUMSEL didukung oleh Subbagian Perencanaan dan Administrasi (Subbag Renmin), Subbidang Teknologi Komunikasi (Subbid Tekkom) dan Subbidang Teknologi Informasi (Subbid Tekinfo) [3].

Subbagian Perencanaan dan Administrasi (Subbag Renmin) merupakan bagian yang berperan dalam menyusun perencanaan program kerja dan anggaran, manajemen personel dan kinerja, serta mengelola keuangan dan pelayanan ketatausahaan dan lingkungan [4]. Subbidang Teknologi Komunikasi (Subbid Tekkom) merupakan bagian yang berperan dalam menyelenggarakan dan membina sistem dan teknologi komunikasi, meliputi pembangunan dan pengembangan jaringan, pelayanan komunikasi, serta pemeliharaan dan perbaikan alat dan infrastruktur jaringan komunikasi [5].

Subbidang Teknologi Informasi (Subbid Tekinfo) di Polda bertugas membina dan menyelenggarakan sistem dan teknologi informasi yang meliputi pengumpulan dan pengolahan data serta penyajian informasi Kamtibmas dan dokumentasi bidang operasional maupun pembinaan, termasuk teknologi informasi komunikasi yang berkaitan dengan sarana dan prasarana [5].

Dalam mendukung pelaksanaan tugas-tugas tersebut, BID TIK POLDA SUMSEL mengandalkan berbagai perangkat dan aplikasi pendukung seperti *Microsoft Office*, lainnya, termasuk pemanfaatan website ASTINA POLRI sebagai bagian dari sistem informasi internal. Namun demikian, di tengah pemanfaatan teknologi informasi, terdapat berbagai risiko yang berpotensi menimbulkan dampak negatif terhadap keberlangsungan sistem, proses, maupun layanan yang disediakan di lingkungan BID TIK POLDA SUMSEL.

Dalam lingkungan BID TIK POLDA SUMSEL, terdapat berbagai risiko yang berpotensi mengganggu sistem, proses, dan layanan. Risiko tersebut antara lain *human error* seperti data yang terhapus atau lupa disimpan, pemadaman listrik mendadak akibat bencana teknologi, gangguan koneksi internet yang sangat bergantung pada jaringan *Wi-Fi* sehingga aktivitas penginputan data terhambat, kerusakan perangkat keras. Risiko lain yang juga pernah terjadi insiden server dipenuhi asap akibat AC ruangan yang mati tanpa terdeteksi, serta aktivitas mencurigikan berupa akses domain oleh banyak IP *address* yang menyerupai serangan spam dan mengganggu kestabilan website. Selain itu, belum tersedia dokumentasi resmi terkait insiden risiko, baik di tingkat individu maupun divisi, yang menjadi kelemahan dalam pengelolaan risiko.

Risiko sendiri dapat diartikan sebagai suatu kondisi ketidakpastian yang dapat menimbulkan konsekuensi merugikan atau membahayakan, baik akibat peristiwa yang sedang berlangsung atau yang berpotensi terjadi [7]. Mengingat banyaknya potensi ancaman risiko yang dihadapi, pengelolaan risiko dalam pemanfaatan teknologi informasi menjadi aspek yang sangat penting. Pengelolaan risiko yang baik akan membantu organisasi dalam menjaga kelangsungan operasional, meminimalkan dampak kerugian, serta meningkatkan kualitas pelayanan kepada masyarakat melalui penerapan pengelolaan risiko teknologi informasi.

Pengelolaan risiko teknologi informasi dapat dilakukan dengan menggunakan salah satu kerangka kerja yang banyak diadopsi oleh organisasi, yaitu COBIT 5 (*Control Objectives for Information and Related Technologies*). COBIT 5 merupakan *framework* tata kelola dan manajemen teknologi informasi yang dapat membantu organisasi dalam mencapai tujuan bisnisnya melalui pengendalian, pengelolaan, dan mitigasi risiko yang terstruktur [8]. Dalam COBIT 5, salah satu domain yang fokus pada pengelolaan risiko adalah domain APO12 (*Manage Risk*).

Domain APO12 (*Manage Risk*) dalam kerangka kerja COBIT 5 berperan dalam memandu organisasi untuk melakukan proses identifikasi, penilaian, dan mitigasi risiko secara sistematis. Pendekatan ini memastikan bahwa pengelolaan risiko dilakukan secara proaktif melalui langkah-langkah yang terdokumentasi, terstruktur, dan terukur [9]. Pemilihan domain APO12 dalam COBIT 5

dilakukan karena domain ini secara spesifik berfokus pada pengelolaan risiko teknologi informasi secara menyeluruh, mulai dari identifikasi hingga mitigasi risiko, serta penyusunan profil risiko yang terdokumentasi. COBIT 5 dipilih karena *framework* ini menyediakan pendekatan kapabilitas yang terukur, telah teruji di banyak organisasi, dan memiliki struktur proses yang lebih stabil dibandingkan versi COBIT 2019 yang lebih kompleks dan belum banyak digunakan di instansi pemerintah.

Selain itu, efektivitas penerapan COBIT 5 domain APO12 telah dibuktikan dalam berbagai penelitian. Salah satunya di PT Perkebunan Nusantara V Pekanbaru menunjukkan bahwa COBIT 5 domain APO12 mencapai tingkat kapabilitas 4 (*Predictable Process*), sementara EDM03 mencapai level 5 (*Optimizing Process*), dengan rekomendasi untuk menyelaraskan pengelolaan risiko dalam proses TI [10].

Penelitian yang pernah dilakukan di BPR Agung Sejahtera menggunakan COBIT 5 domain APO12 menunjukkan tingkat kapabilitas pada level 1 (*Performed Process*), dengan rekomendasi peningkatan ke level 2 [11]. Penelitian di UPT-TIK Universitas Brawijaya menggunakan COBIT 5 domain APO12 menemukan bahwa tingkat kapabilitas manajemen risiko berada pada level 0, menyoroti perlunya pengembangan kebijakan dan prosedur standar [12].

Selain itu, penelitian serupa dalam analisis di layanan pengunduran diri mahasiswa di Universitas Ahmad Dahlan menggunakan COBIT 5 domain APO12 untuk mengidentifikasi dan mengelola risiko yang dapat mempengaruhi kualitas layanan akademik [13]. Pemilihan COBIT 5 domain APO12 dalam penelitian manajemen risiko teknologi informasi didasarkan pada kekuatan struktur prosesnya yang komprehensif, penerapannya yang luas di berbagai sektor, serta kemampuannya dalam membantu organisasi menilai tingkat kapabilitas manajemen risiko yang selaras dengan tujuan bisnis dan kebutuhan pengembangan berkelanjutan.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengidentifikasi potensi ancaman risiko teknologi informasi yang dapat menimbulkan kerugian atau dampak negatif di lingkungan BID TIK POLDA SUMSEL. Penelitian ini akan memberikan rekomendasi pengelolaan risiko berbasis *framework* COBIT 5, khususnya pada domain APO12 (*Manage Risk*), serta menganalisis tingkat kapabilitas pengelolaan risiko teknologi informasi melalui pendekatan proses COBIT 5 domain APO12 (*Manage Risk*), baik dalam kondisi saat ini (*As Is*) maupun kondisi yang diharapkan di masa depan (*To Be*). Dengan demikian, penelitian ini diharapkan dapat memberikan evaluasi yang mendalam mengenai manajemen risiko yang ada, serta memberikan solusi yang dapat membantu BID TIK POLDA SUMSEL dalam menangani risiko teknologi informasi secara lebih efektif.

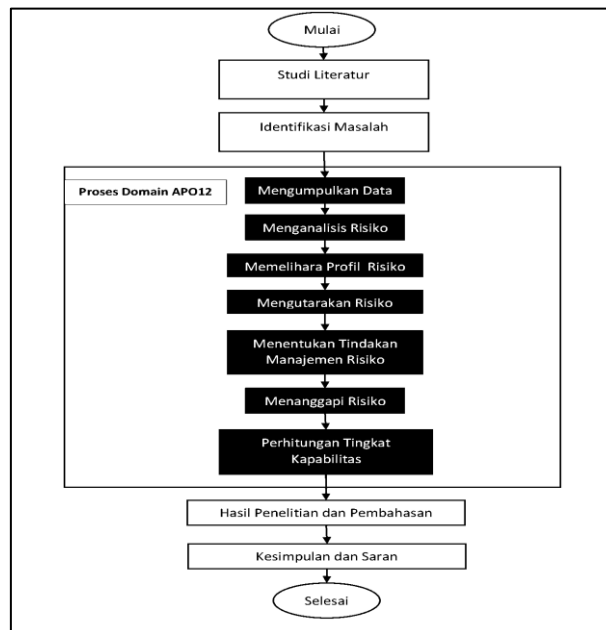
Metode Penelitian

A. Studi Literatur

Mengumpulkan data pustaka, membaca dan mencatat, serta mengelolah bahan penelitian. Penelitian terdahulu, buku-buku yang berkaitan dengan COBIT 5 Domain APO12 (*Manage Risk*).

B. Identifikasi Masalah

Mengidentifikasi masalah pada BID TIK POLDA SUMSEL terkait dengan risiko teknologi informasi seperti *human error* seperti data yang terhapus atau lupa disimpan, pemadaman listrik mendadak akibat bencana teknologi, gangguan koneksi internet yang sangat bergantung pada jaringan *Wi-Fi*, kerusakan perangkat keras. Risiko lain yang juga pernah terjadi insiden server dipenuhi asap akibat AC ruangan yang mati tanpa terdeteksi, serta aktivitas mencurigakan berupa akses domain oleh banyak IP *address* yang menyerupai serangan spam dan mengganggu kestabilan website. Selain itu, belum tersedia dokumentasi resmi terkait insiden risiko, baik di tingkat individu maupun divisi, yang menjadi kelemahan dalam pengelolaan risiko.



Gambar 1 Kerangka Penelitian

C. APO12.01 Mengumpulkan Data

- Mengumpulkan data mengenai lingkungan internal di BID TIK POLDA SUMSEL.
- Mengumpulkan data terkait kejadian risiko yang pernah dialami dan berpotensi menimbulkan dampak terhadap manfaat dari penerapan teknologi informasi.
- Menganalisis pengalaman terjadinya risiko teknologi informasi yang akan dilakukan berdasarkan wawancara, kuesioner *capability level* dan observasi pada BID TIK POLDA SUMSEL pada Subbagian Renmin, Subbid Tekkom dan Subbid Tekinfo.

D. APO12.02 Menganalisis Risiko

- Menganalisis dampak terjadinya risiko dan mempertimbangkan semua faktor risiko di BID TIK POLDA SUMSEL.
- Membangun harapan terhadap adanya pengendalian, kemampuan mendeteksi dan respon yang tepat terhadap risiko.
- Memperkirakan kemungkinan dan dampak kerugian atau keuntungan akibat risiko teknologi informasi.

E. APO12.03 Memelihara Profil Risiko

- Secara berkala, menggabungkan semua informasi profil risiko ke dalam satu profil risiko keseluruhan.
- Kumpulan kejadian risiko teknologi informasi yang telah terjadi dicatat dalam profil risiko teknologi informasi di BID TIK POLDA SUMSEL.

F. APO12.04 Mengutarakan Risiko

Hasil analisis risiko dituangkan dalam dokumen yang tersedia untuk memperbarui profil risiko organisasi. Pelaporan dilakukan secara sistematis dan terstruktur guna memastikan seluruh pihak memahami dan mengidentifikasi risiko yang dihadapi oleh BID TIK POLDA SUMSEL secara komprehensif.

G. APO12.05 Menentukan Tindakan Manajemen Risiko

Tindakan manajemen risiko dilakukan dengan mempertahankan kontrol yang telah diterapkan guna memastikan pengelolaan risiko berjalan efektif. Proses ini mencakup pemantauan berkelanjutan, penerapan prosedur pengendalian, dan penyesuaian terhadap batas toleransi risiko yang telah ditentukan. Klasifikasi risiko juga mempertimbangkan kemungkinan adanya tumpang tindih antar

risiko dalam sistem TI yang telah diidentifikasi. Upaya manajemen risiko yang dilakukan oleh BID TIK POLDA SUMSEL diharapkan dapat meningkatkan kesiapan dalam menghadapi potensi ancaman serta menjaga kesinambungan dan keberhasilan operasional secara berkelanjutan.

H. APO12.06 Menanggapi Risiko

Proses ini mencakup pengembangan serta penerapan prosedur untuk menangani situasi berisiko secara efektif, disertai dengan penyusunan rencana pengujian yang mendokumentasikan langkah-langkah penanganan insiden. Uji rencana tersebut disusun secara sistematis dan terstruktur guna memastikan BID TIK POLDA SUMSEL mampu merespons secara cepat dan tepat saat risiko terjadi.

I. Perhitungan Tingkat Kapabilitas

Dalam penelitian ini digunakan skala Likert untuk mengukur sikap, persepsi, dan pendapat responden. Skala ini dikembangkan oleh Rensis Likert dan umum digunakan untuk mengkuantifikasi data kualitatif menjadi data kuantitatif (Sugiyono, 2009). Penentuan nilai kapabilitas APO12 menggunakan skala Likert, dihitung untuk kondisi *As Is* dan *To Be* dengan rumus konversi dari hasil kuesioner pada Persamaan 1.

$$NK = \frac{(Nk \times LP)a + (Nk \times LP)b + (Nk \times LP)c + (Nk \times LP)d + (Nk \times LP)e + (Nk \times LP)f}{100} \dots\dots\dots (1)$$

Keterangan:

*NK : Nilai kapabilitas

*LP : Level *percentage* (pada setiap distribusi jawaban kuesioner *capability level*).

*Nk : Nilai kapabilitas yang tertera pada tabel tingkat kapabilitas.

Penilaian tingkat kapabilitas teknologi informasi berdasarkan proses domain APO12 dalam manajemen risiko teknologi informasi mencakup kondisi saat ini (*As Is*) dan kondisi yang diharapkan (*To Be*). Berikut merupakan nilai ketetapan kapabilitas COBIT 5 dapat dilihat pada Tabel 1.

Tabel 1 Tingkat Kapabilitas

Rentang Nilai	Level	Nilai Kapabilitas	Tingkat Kapabilitas
0 – 0,50	0	0,00	0 <i>Non-Existent</i>
0,51 – 1,50	1	1,00	1 <i>Performed Process</i>
1,51 – 2,50	2	2,00	2 <i>Manage Process</i>
2,51 – 3,50	3	3,00	3 <i>Established Process</i>
3,51 – 4,50	4	4,00	4 <i>Predictable Process</i>
4,51 – 5,00	5	5,00	5 <i>Optimising Process</i>

Hasil dan Pembahasan

A. Hasil Penelitian

1. Proses Domain APO12

a. Aktivitas APO12. 01 (Mengumpulkan Data)

Kasubbag Perencanaan dan Administrasi (Subbag Renmin), Kasubbid Subbidang Teknologi Komunikasi (Subbid Tekkom), Kasubbid Teknologi Informasi (Subbid Tekinfo) yang masing-masing menghadapi risiko yang berbeda. Terdapat faktor yang penyebab Gambar 2.1 dan kemungkinan risiko yang didapatkan. Adapun bagian, faktor dan kemungkinan risiko yaitu pada Tabel 2.

Tabel 2 Pengumpulan Data

Bagian	Faktor	Kemungkinan Risiko
Subbag Renmin	Sumber Daya Manusia	<i>Human Error</i>
	Alam/Lingkungan	Pemadaman listrik mendadak
	Keamanan	Serangan <i>spam</i>
Subbid Tekkom	Sistem dan Infrastruktur	Gangguan koneksi internet Kerusakan perangkat keras
Subbid Tekinfo	Alam/Lingkungan	Server dipenuhi asap saat AC mati tanpa terdeteksi
	Data dan Informasi	Tidak ada dokumen resmi insiden risiko

b. Aktivitas APO12.02 (Menganalisis Risiko)

Tahapan analisis risiko diawali dengan proses identifikasi terhadap potensi risiko yang berpeluang terjadi, dilanjutkan dengan penilaian terhadap tingkat dampak yang dapat ditimbulkannya. Penilaian ini mencakup evaluasi terhadap probabilitas terjadinya risiko dan besarnya konsekuensi yang ditimbulkan. Hasil analisis tersebut disajikan dalam Tabel 3.

Tabel 3 Menganalisis Risiko

Faktor	Kemungkinan Risiko	Peluang Kejadian Risiko	Dampak
Sumber Daya Manusia	<i>Human Error</i>	Kadang-kadang	Sedang
	Pemadaman listrik	Kadang-kadang	Besar
Alam/Lingkungan	Server dipenuhi asap saat AC mati tanpa terdeteksi	Jarang	Besar
	Gangguan koneksi internet	Sering	Sedang
Sistem dan Infrastruktur	Kerusakan perangkat keras	Kadang-kadang	Besar
Keamanan	Serangan <i>spam</i>	Jarang	Besar
Data dan Informasi	Tidak ada dokumen resmi insiden risiko	Sering	Sedang

c. Aktivitas APO12.03 (Memelihara Profil Risiko)

Dalam kegiatan pemeliharaan profil risiko, informasi dikumpulkan melalui proses pengumpulan data dan analisis risiko untuk mengevaluasi tingkat risiko yang ada. Diklasifikasikan berdasarkan kategori tingkat risiko dan dampak risiko, sebagaimana ditampilkan dalam Tabel 4.

Tabel 4 Hasil Tahapan Pemeliharaan Profil Risiko

Kemungkinan Risiko	Penyebab Risiko	Tingkat Risiko	Dampak Risiko
<i>Human Error</i>	Kurangnya pelatihan dan tidak ada SOP	Sedang	Data hilang, gangguan operasional
Pemadaman listrik	Tidak ada backup listrik	Besar	Sistem mati, layanan terhenti
Server dipenuhi asap saat AC mati tanpa terdeteksi	Sensor suhu tidak aktif	Besar	Kerusakan sever dan Data
Gangguan koneksi internet	Provider bermasalah	Sedang	Tidak bisa mengakses sistem

Kemungkinan Risiko	Penyebab Risiko	Tingkat Risiko	Dampak Risiko
Kerusakan perangkat keras	Perangkat tua dan kurang perawatan rutin	Besar	<i>Downtime</i> operasional
Serangan <i>spam</i>	Gangguan pada website akibat aktivitas mencurigakan berupa akses domain oleh sejumlah besar alamat IP secara bersamaan	Besar	<i>Distributed Denial of Service</i> (DDoS)
Tidak ada dokumen resmi insiden risiko	Tidak ada kebijakan dokumentasi	Sedang	Analisis risiko tidak valid

d. Aktivitas APO12.04 (Mengutarakan Risiko)

Dalam kegiatan komunikasi risiko, proses ini melibatkan penyampaian informasi mengenai risiko yang telah diidentifikasi beserta kemungkinan terjadinya. Selain itu, disusun rekomendasi strategis untuk mengelola dan meminimalkan dampak yang mungkin terjadi pada Tabel 5.

Tabel 5 Mengutarakan Risiko

Kemungkinan Risiko	Peluang	Penyebab Risiko	Tingkat Risiko	Dampak Risiko	Rekomendasi Strategis
<i>Human Error</i>	Kadang-kadang	Kurangnya pelatihan dan tidak ada SOP	Sedang	Data hilang, gangguan operasional	Adakan pelatihan rutin dan SOP jelas
Pemadaman listrik	Kadang-kadang	Tidak ada backup listrik	Besar	Sistem mati, layanan terhenti	Siapkan UPS dan genset
Server dipenuhi asap saat AC mati tanpa terdeteksi	Jarang	Sensor suhu tidak aktif	Besar	Kerusakan sever dan Data	Pasang detektor asap dan sistem ventilasi
Gangguan koneksi internet	Sering	Provider bermasalah	Sedang	Tidak bisa mengakses sistem	Gunakan koneksi internet cadangan
Kerusakan perangkat keras	Kadang-kadang	Perangkat tua dan kurang perawatan rutin	Besar	<i>Downtime</i> operasional	Lakukan perawatan rutin perangkat
Serangan <i>spam</i>	Jarang	Gangguan pada website akibat aktivitas mencurigakan berupa akses domain oleh sejumlah besar alamat IP secara bersamaan	Besar	<i>Distributed Denial of Service</i> (DDoS)	Menerapkan <i>Web Application Firewall</i> (WAF) dan sistem deteksi serangan DDoS untuk secara proaktif menyaring lalu lintas mencurigakan sebelum mencapai server utama.
Tidak ada dokumen resmi insiden risiko	Sering	Tidak ada kebijakan dokumentasi	Sedang	Analisis risiko tidak valid	Buat dan terapkan format pelaporan

e. Aktivitas APO12.05 (Menentukan Tindakan Manajemen Risiko)

Langkah selanjutnya adalah menentukan tindakan manajemen risiko berdasarkan risiko dan tingkat risiko yang ada pada Tabel 6. Pada tahap ini, organisasi menentukan langkah atau strategi yang paling tepat untuk mengelola setiap risiko sesuai tingkat risikonya.

Tabel 6 Menentukan Tindakan Manajemen Risiko

Risiko	Tingkat Risiko	Tindakan Manajemen Risiko
<i>Human Error</i>	Sedang	Adakan pelatihan rutin dan SOP jelas
Pemadaman listrik	Besar	Siapkan UPS dan genset
Server dipenuhi asap saat AC mati tanpa terdeteksi	Besar	Pasang detektor asap dan sistem ventilasi
Gangguan koneksi internet	Sedang	Gunakan koneksi internet cadangan
Kerusakan perangkat keras	Besar	Lakukan perawatan rutin perangkat
Serangan <i>spam</i>	Besar	Menerapkan <i>Web Application Firewall</i> (WAF) dan sistem deteksi serangan DDoS untuk secara proaktif menyaring lalu lintas mencurigakan sebelum mencapai server utama.

f. Aktivitas APO12.06 (Menanggapi Risiko)

Penanganan risiko dilakukan dengan menerapkan respons atau rekomendasi yang telah ditentukan, berdasarkan evaluasi kerugian sebelumnya. Hasilnya digunakan untuk menyusun profil risiko dan tindakan mitigasi, khususnya pada aspek TI. Aktivitas meliputi pelaporan risiko kepada stakeholder serta penyimpanan data untuk mencegah risiko terulang. Tindakan yang digunakan meliputi: Menghindari risiko, Berbagi risiko (transfer), Mitigasi risiko, Menerima risiko. Langkah-langkah mitigasi tiap subbagian disajikan pada Tabel 7.

Tabel 7 Menanggapi Risiko

Risiko	Tingkat Risiko	Menangani Risiko
Human Error	Sedang	Mengurangi kemungkinan terjadinya risiko atau dampaknya melalui perlakuan yang sesuai (Mitigasi)
Pemadaman listrik	Besar	Mengurangi kemungkinan atau dampak risiko dengan membagi atau mentransfer risiko tersebut (Berbagi risiko).
Server dipenuhi asap saat AC mati tanpa terdeteksi	Besar	Mengurangi kemungkinan terjadinya risiko atau dampaknya melalui perlakuan yang sesuai (Mitigasi)
Gangguan koneksi internet	Sedang	Mengurangi kemungkinan atau dampak risiko dengan membagi atau mentransfer risiko tersebut (Berbagi risiko).
Kerusakan perangkat keras	Besar	Mengurangi kemungkinan terjadinya risiko atau dampaknya melalui perlakuan yang sesuai (Mitigasi)
Serangan spam	Besar	Menghindari Risiko
Tidak ada dokumen resmi insiden risiko	Sedang	Tidak mengambil tindakan risiko tersebut (Menerima risiko).

2. Perhitungan Tingkat Kapabilitas

Perhitungan tingkat kapabilitas merupakan untuk menghitung kondisi saat ini (*As Is*) dan kondisi diharapkan (*To Be*). Perhitungan menggunakan rumus Persamaan 1 masing-masing subdomain APO12 dari 1 sampai 6. Adapun perhitungan nilai kapabilitas *As Is* dan *To Be* pada Tabel 8.

Tabel 8 Perhitungan Nilai Kapabilitas *As Is* dan *To Be* APO12

Status APO12.01	Nk x LP						Total Nk x LP/100	NK	Level
	0	1	2	3	4	5			
<i>As Is</i>	0.0	1.0	12.0	9.0	80.0	100.0	202.0	2.02	2
<i>To Be</i>	0.0	0.0	0.0	0.0	96.0	225.0	321.0	3.21	3
Status APO12.02	Nk x LP						Total Nk x LP/100	NK	Level
	0	1	2	3	4	5			
<i>As Is</i>	0.0	3.0	0.0	45.0	112.0	75.0	235.0	2.35	2
<i>To Be</i>	0.0	0.0	0.0	0.0	64.0	350.0	414.0	4.14	4
Status APO12.03	Nk x LP						Total Nk x LP/100	NK	Level
	0	1	2	3	4	5			
<i>As Is</i>	0.0	3.0	0.0	0.0	96.0	150.0	249.0	2.49	2
<i>To Be</i>	0.0	0.0	0.0	0.0	0.0	450.0	450.0	4.5	4
Status APO12.04	Nk x LP						Total Nk x LP/100	NK	Level
	0	1	2	3	4	5			
<i>As Is</i>	0.0	5.0	0.0	0.0	48.0	175.0	228.0	2.28	2
<i>To Be</i>	0.0	0.0	0.0	0.0	0.0	350.0	350.0	3.5	3
Status APO12.05	Nk x LP						Total Nk x LP/100	NK	Level
	0	1	2	3	4	5			
<i>As Is</i>	0.0	2.0	0.0	0.0	48.0	75.0	125.0	1.25	1
<i>To Be</i>	0.0	0.0	0.0	0.0	0.0	225.0	225.0	2.25	2
Status APO12.06	Nk x LP						Total Nk x LP/100	NK	Level
	0	1	2	3	4	5			
<i>As Is</i>	0.0	3.0	4.0	0.0	0.0	200.0	207.0	2.07	2
<i>To Be</i>	0.0	0.0	0.0	0.0	0.0	300.0	300.0	3	3
Rata-rata							<i>As Is</i>	<i>To Be</i>	Level
							<i>As Is</i>	<i>To Be</i>	
							2,07	3,43	2 3

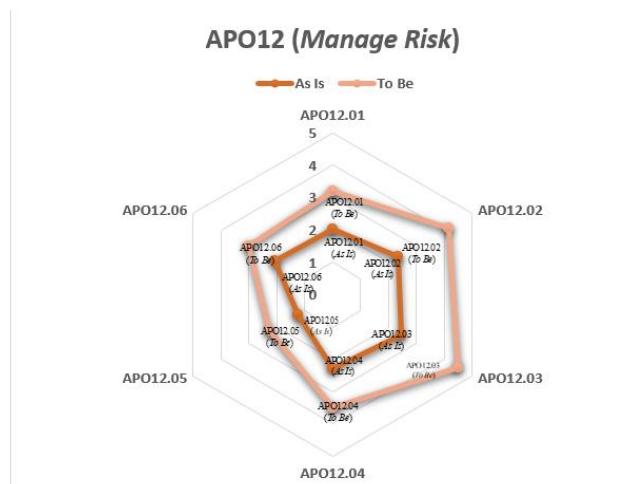
- Nilai Kapabilitas APO12.01 (Mengumpulkan Data)
Menunjukkan bahwa proses pengumpulan data risiko sudah mulai berjalan secara terstruktur namun masih dapat ditingkatkan dari sisi integrasi dan dokumentasi lintas unit.
- Nilai Kapabilitas APO12.02 (Menganalisis Risiko)
Institusi menargetkan analisis risiko yang lebih mendalam, terukur, dan terdokumentasi penuh secara lintas unit.
- Nilai Kapabilitas APO12.03 (Memelihara Profil Risiko)
Menunjukkan adanya komitmen untuk menjadikan profil risiko sebagai dokumen hidup yang digunakan untuk perencanaan dan pengambilan keputusan.
- Nilai Kapabilitas APO12.04 (Mengutarakan Risiko)
Menunjukkan bahwa proses pelaporan sudah dilaksanakan, namun masih membutuhkan peningkatan, khususnya dalam hal standarisasi serta perluasan jangkauan komunikasi risiko secara menyeluruh, baik secara *horizontal* antarunit maupun *vertikal* kepada pimpinan.
- Nilai Kapabilitas APO12.05 (Menentukan Tindakan Manajemen Risiko)
Organisasi sedang dalam proses memperkuat peran Kasub agar lebih proaktif dan terdokumentasi dalam menentukan tindakan mitigasi risiko.
- Nilai Kapabilitas APO12.06 (Menanggapi Risiko)
Menunjukkan bahwa proses penanggulangan risiko sudah mulai terbentuk, dan ke depan akan diarahkan menjadi lebih sistematis, terdokumentasi, dan dapat dievaluasi.

Berdasarkan hasil penelitian, nilai *As Is* sebesar 2,07 menunjukkan kapabilitas berada di Level 2, yaitu proses manajemen risiko telah dijalankan dan dikelola, namun belum terdokumentasi secara formal dan belum konsisten. Sementara itu, nilai *To Be* sebesar 3,43 menargetkan Level 3, di mana proses pengurangan risiko diharapkan sudah terdokumentasi dan diterapkan secara terstruktur untuk mencapai hasil yang konsisten.

3. Grafik Proses APO12 (*Manage Risk*)

Grafik Proses APO12 menunjukkan adanya kesenjangan yang jelas antara kondisi saat ini (*As Is*) dan target yang diharapkan (*To Be*) pada seluruh subproses. Nilai rata-rata *As Is* sebesar 2,07 (Level 2) menunjukkan bahwa proses sudah berjalan namun belum terdokumentasi secara konsisten. Sementara itu, nilai rata-rata *To Be* sebesar 3,43 (Level 3) menargetkan proses yang terdokumentasi, distandardisasi, dan dijalankan secara konsisten. Gap ini menunjukkan perlunya peningkatan dalam dokumentasi dan koordinasi antarunit. Pada subproses APO12.01 (Mengumpulkan Data), dokumentasi yang belum optimal (*As Is* 2,02) menghambat analisis lanjutan pada APO12.02 (Menganalisis Risiko) yang menargetkan Level 4.

Subproses APO12.03 (Memelihara Profil Risiko) juga menunjukkan kesenjangan besar (*As Is* 2,46 – *To Be* 4,5), yang mencerminkan keterbatasan dalam pemanfaatan data risiko untuk pengambilan keputusan. Subproses APO12.04 (*Mengutarakan Risiko*) masih berada di Level 2, menunjukkan perlunya peningkatan standar komunikasi risiko. APO12.05 (Menentukan Tindakan Manajemen Risiko) memiliki kesenjangan paling besar (*As Is* 1,25 – *To Be* 2,25), menandakan proses masih bersifat reaktif dan minim dokumentasi. Sedangkan APO12.06 (Menanggapi Risiko) menunjukkan perlunya sistem respons risiko yang lebih terstruktur dan terdokumentasi. Secara keseluruhan, kelemahan utama terletak pada dokumentasi yang belum memadai di awal proses. Oleh karena itu, perbaikan sebaiknya difokuskan pada penguatan dokumentasi pada tahap APO12.01, karena berdampak langsung terhadap efektivitas proses-proses berikutnya. Dengan menutup gap ini, BID TIK POLDA SUMSEL dapat membangun sistem manajemen risiko TI yang lebih kuat, terstruktur, dan berkelanjutan.



Gambar 2 Grafik Proses APO12 (*Manage Risk*)

B. Pembahasan

a. APO12.01 (Mengumpulkan Data)

Nilai *As Is* sebesar 2,02 menunjukkan proses pengumpulan data sudah berjalan, namun dokumentasinya belum optimal. Hal ini menjadi hambatan awal yang berdampak pada subproses berikutnya yang paling prioritas, agar dapat segera ditangani melalui langkah-langkah penanganan yang tepat.

b. APO12.02 (Menganalisis Risiko)

Menargetkan Level 4, namun belum tercapai karena kurangnya data yang terdokumentasi dari proses sebelumnya. Analisis belum sepenuhnya mendalam dan lintas unit.

c. APO12.03 (Memelihara Profil Risiko)

Terdapat kesenjangan besar (*As Is* 2,46 – *To Be* 4,5) yang menandakan bahwa data risiko belum dimanfaatkan maksimal dalam pengambilan keputusan..

d. APO12.04 (Mengutarakan Risiko)

Masih berada di Level 2. Proses pelaporan sudah dilakukan, namun belum memenuhi standar komunikasi risiko yang konsisten antarunit dan ke pimpinan.

e. APO12.05 (Menentukan Tindakan Manajemen Risiko)

Memiliki gap terbesar (*As Is* 1,25 – *To Be* 2,25). Proses masih bersifat reaktif dan belum terdokumentasi secara sistematis.

f. APO12.06 (Menanggapi Risiko)

Perlu perbaikan dalam struktur dan dokumentasi respons risiko agar lebih terukur dan dapat dievaluasi secara berkelanjutan.

Kesimpulan

Kesimpulan dari penelitian ini mengenai analisis dan penilaian risiko pada BID TIK POLDA SUMSEL menggunakan *framework* COBIT 5, yaitu:

1. Tingkat kapabilitas manajemen risiko TI pada BID TIK POLDA SUMSEL saat ini (*As Is*) berada pada rata-rata level 2,07, yang menunjukkan bahwa proses telah dikelola namun belum sepenuhnya terdokumentasi dan konsisten. Kondisi yang diharapkan (*To Be*) memiliki rata-rata pada level 3,43, dengan target mencapai Level 3 (*Established Process*), yaitu proses yang telah ditetapkan secara formal, terdokumentasi, serta dijalankan secara terstruktur dan berkelanjutan.
2. Setiap subbagian di bawah BidTIK (Kasub Subbag Renmin, Kasub Subbid Tekkom, dan Kasub Subbid Tekinfo) telah berperan aktif dalam implementasi manajemen risiko, namun masih diperlukan perbaikan dalam hal dokumentasi, pelaporan, dan koordinasi lintas unit. Adanya selisih antara kondisi *As Is* dan *To Be* menjadi indikator penting perlunya peningkatan kapabilitas untuk mencapai tata kelola risiko TI yang optimal di lingkungan BID TIK POLDA SUMSEL.

Saran

1. BID TIK POLDA SUMSEL menyusun dan mengimplementasikan standar operasional prosedur (SOP) yang terstruktur untuk pengelolaan risiko teknologi informasi, meliputi identifikasi, analisis, pelaporan, dan penanganan risiko. Langkah ini penting agar seluruh proses dapat dijalankan secara konsisten di setiap subunit.
2. Diharapkan penelitian ke depan dapat memperluas cakupan dengan menilai domain lain dalam COBIT 5, seperti DSS (*Deliver, Service, and Support*) atau MEA (*Monitor, Evaluate, and Assess*), serta menggunakan pendekatan kualitatif untuk mengeksplorasi hambatan dan faktor keberhasilan implementasi manajemen risiko TI secara lebih mendalam.

Daftar Pustaka

- [1] Afif Khoirul Abdi, Endro Kuswoyo dan Indah Purnamasari. 2022. Evaluasi Sistem Informasi Electronic Daily Perform Report (E-Dpr) Dengan Menggunakan Framework COBIT 5. *Jurnal Informasi Dan Komputer*, Vol 101 No. 2. doi: 0.33998/mediasisfo.2020.14.1.766
- [2] Cava Billa Al Husaini. 2023. Pemahaman Resiko Dan Manajemen Resiko. *Jurnal Nuansa: Publikasi Ilmu Manajemen Dan Ekonomi Syariah*, Vol 1 No. 3. doi: sdoi.org/10.61132/nuansa.v1i3.272
- [3] Rievaldy Ardhyka, Afifah Fidaiyah dan Ruci Meiyanti. 2023. Analisis Manajemen Risiko IT Menggunakan COBIT5 Pada Domain APO12. *Jurnal Informasi Dan Teknologi*, Vol 5 No. 2. doi: doi.org/10.37034/jidt.v5i2.325
- [4] Muhammad Abdul Azis dan Ani Yoraeni. 2023. Audit Sistem Informasi Persediaan Barang di PT. Karoseri Jaya Mandiri Menggunakan Framework Cobit 5. *Jurnal Ilmu Komputer Dan Bisnis*,

- Vol 14 No. 2. doi: doi.org/10.30656/jsii.v12i1.9771
- [5] Nathanael Budiono, Ariya Dwika Cahyono dan Penidas Fiodinggo Tanaem. 2021. Evaluasi Manajemen Risiko Teknologi Informasi Pada Perusahaan Daerah Air Minum Kota Salatiga Menggunakan Framework Cobit 5.0. *Sebatik*, Vol 5 No. 1. doi: doi.org/10.46984/sebatik.v25i1.1174
 - [6] Novitasari Butarbutar1, Andeka Rocky Tanaamah. 2021. Analisis Manajemen Risiko Menggunakan COBIT 5 Domain APO12 (Studi Kasus: Yayasan Bina Darma). *Journal of Information Systems and Informatics*, Vol 3 No. 3. doi: 10.51519/journalisi.v3i3.155
 - [7] Yunike, Yaulie Rindaengan dan Steven Sentinuwo. 2021. Penerapan Cobit 5 Build, Acquire and Implement Untuk Mengukur Kematangan Dinas Komunikasi Dan Informatika Kota Manado. *Jurnal Teknik Elektro Dan Komputer*, Vol 1 No. 8. doi: https://repo.unsrat.ac.id/3082/
 - [8] Furiansyah Dipraja, Rifqi Syamsul Fuadi dan Tonton Taufik Rachman. 2021. Implementasi Manajemen Risiko Sistem Administrasi Layanan Akademik Menggunakan Framework COBIT 5.0. *INTERNAL (Information System Journal)*, Vol 4 No. 2. doi: doi.org/10.32627/internal.v4i2.395
 - [9] Joshua Ecneas dan Augie David Manuputty. 2021. Analisis Manajemen Risiko Teknologi Informasi Software PEGA Menggunakan ISO 31000. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, Vol 8 No. 1. doi: 10.35957/jatisi.v8i1.601
 - [10] Ridho Fahlepi, Mona Fronita, Eki Saputra, Muhammad Luthfi Hamzah, Arif Marsal dan Suandi Daulay. 2023. Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000. *Jurnal Sains Komputer & Informatika (J-SAKTI)*, Vol 7 No. 2. doi: dx.doi.org/10.30645/j-sakti.v7i2.675
 - [11] Al Fajri, Novriyanto, Nazruddin Safaat dan Muhammad Affandes. 2023. Analisis Manajemen Risiko TI Menggunakan Framework COBIT 5 Domain APO12 dan EDM03. *KLIK: Kajian Ilmiah Informatika Dan Komputer*, Vol 4 No. 3. doi: doi.org/10.30865/klik.v4i3.1396
 - [12] Fereria Anindya. 2024. Manajemen Risiko Teknologi Informasi Pada PT. Hagen Amersa Veta Menggunakan Framework COBIT 5. *Jurnal Science Sistem Informasi*, Vol 2 No. 3. doi: dx.doi.org/10.31602/jsii.v2i3.16337
 - [13] Muhammad Nur Fuad dan Imam Riadi. 2020. Risk Management Assessment on Human Resource Information Technology Services using COBIT 5. *International Journal of Computer Applications*, Vol 175 No. 23. doi: 10.5120/ijca2020920756
 - [14] Nyimas Hamidah Purnama Agustriani dan Tata Sutabri. 2024. Analisis Domain Deliver, Service dan Support Untuk Pengukuran Kualitas Layanan E-Government Menggunakan Framework Cobit 5.0. *Journal of Information Technology Ampera*, Vol 5 No. 1. doi:10.51519/journalita.v5i1.514
 - [15] ISACA. (2013). *COBIT 5 For Risk*. ISACA.
 - [16] Andri Wijaya. 2023. Penyelarasan Tujuan dan Sasaran Bisnis Teknologi Informasi Menggunakan Kerangka Kerja COBIT 4,1. *Jurnal Sistem dan Teknologi Informasi Komunikasi*. Vol 7 No. 1. doi: 10.32524/jusitik.v7i1.1037
 - [17] Steni Laus Aditya, Yohanes Agung Apriyanto, Sri Andayani. 2024. Analisis Manajemen Risiko pada CV. Tunas Mandiri. *Jurnal Sains Sistem Informasi*. Vol 2 No. 2. doi: dx.doi.org/10.31602/jsii.v2i2.14620
 - [18] Thomas Filikano, Andronikus Gunawan, Sri Andayani. 2024. Analisis Risiko Sistem Informasi Akuntansi Menggunakan ISO 31000: 2018 di PT. XYZ. *Jurnal Ilmiah Sistem Informasi*. Vol 4 No. 1. doi: 10.46306/sm.v4i1.71
 - [19] Mutia Maharani, Andreas Klasanto, Bima Apriyanto Simanjuntak dan Sri Andayani. 2025. Manajemen risiko teknologi informasi pada PT. XYZ menggunakan framework COBIT 5. *IT-Explore: Jurnal Penerapan Teknologi Informasi Dan Komunikasi*, Vol 4 No. 2, doi: doi.org/10.24246/itexplore.v4i2.2025.pp173-185