TESIS

EVALUASI MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019

(Studi Kasus: Kantor DPRD Kota Sorong)

disusun oleh

FAJAR MAULANA AHSAN ABBAS

23.51.2492

Konsentrasi : Digital Transformation Intelligence

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

TESIS

EVALUASI MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019

(Studi Kasus: Kantor DPRD Kota Sorong)

EVALUATION OF INFORMATION TECHNOLOGY RISK MANAGEMENT USING THE COBIT 2019 FRAMEWORK

(Case Study: Sorong City DPRD Office)

Diajukan untuk memenuhi salah satu syarat mencapai derajat Pascasarjana

Program Studi S2 Informatika

disusun oleh

FAJAR MAULANA AHSAN ABBAS

23.51.2492

Konsentrasi : Digital Transformation Intelligence

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

EVALUASI MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019

(Studi Kasus: Kantor DPRD Kota Sorong)

EVALUATION OF INFORMATION TECHNOLOGY RISK MANAGEMENT USING THE COBIT 2019 FRAMEWORK

(Case Study: Sorong City DPRD Office)

yang disusun dan diajukan oleh

Fajar Maulana Ahsan Abbas

23.51.2492

telah disetujui oleh Dosen Pembimbing Tesis
pada tanggal 2 Oktober 2025

Dosen Pembimbing,

Alva Hendi Muhammad, S.T., M.Eng., Ph.D

NIK. 190302493

HALAMAN PENGESAHAN

EVALUASI MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019
(Studi Kasus: Kantor DPRD Kota Sorong)

EVALUATION OF INFORMATION TECHNOLOGY RISK MANAGEMENT USING THE COBIT 2019 FRAMEWORK
(Case Study: Sorong City DPRD Office)

yang disusun dan diajukan oleh

Fajar Maulana Ahsan Abbas

23.51.2492

Telah dipertahankan di depan Dewan Penguji
pada tanggal 2 Oktober 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Hanif Al Fatta, S.Kom., M.Kom.,Ph.D. **NIK. 190302096**	
Robert Marco, S.T., M.T., Ph.D. **NIK. 190302228**	
Alva Hendi Muhammad, S.T., M.Eng., Ph.D. **NIK. 190302493**	

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer
Tanggal 2 Oktober 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Fajar Maulana Ahsan Abbas
NIM : 23.51.2492
Konsentrasi : Digital Transformation Intelligence

Menyatakan bahwa Tesis dengan judul berikut:
Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: Kantor DPRD Kota Sorong)

Dosen Pembimbing Utama : Alva Hendi Muhammad, S.T., M.Eng., Ph.D.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, 2 Oktober 2025
Yang Menyatakan,

Fajar Maulana Ahsan Abbas

HALAMAN PERSEMBAHAN

Karya ini saya persembahkan kepada:

1) Saya sendiri, yang telah berjuang dan kuat sampai sekarang, kau keren sobat.
2) Bapak Drs H. Kumisi Abbas M.Si dan Ibu Hj. Nur Asiah, S.KM orang tua saya yang telah membesarkan, membimbing, dan merawat saya hingga menjadi seperti sekarang. Orang tua saya yang selalu memberikan doa, dukungan dan segalanya buat saya.
3) Ir. Ahmad Rithauddin Abbas, ST., Muhammad Nur Adnan Abbas, ST, M.Sc., Nirmala Abbas, S.Si, Apt. dan Ibnu Mukhlis Usman Abbas S.T.Han, M.Ap. kakak-kakak saya yang selalu mendukung, membantu, dan memberikan kasih sayang sebagai seorang kakak.
4) Universitas Amikom Yogyakarta, almamater kebanggaan saya dalam menimba ilmu.
5) Semua pihak yang telah membantu saya, memberikan dukungan dan semangat kepada saya sampai saat ini.

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur kehadirat Allah SWT atas berkat rahmat dan karunia-Nya, Tugas Akhir Skripsi dalam rangka untuk memenuhi sebagian persyaratan untuk mendapatkan gelar Master Komputer Program Studi S2 Informatika, Program Pasca Sarjana Universitas AMIKOM Yogyakarta dengan judul "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: Kantor DPRD Kota Sorong)" dapat disusun sesuai dengan harapan. Tugas akhir Tesis ini dapat diselesai tidak lepas dari bantuan dan kerjasama dengan pihak lain. Berkenaan dengan hal tersebut, penulis ingin menyampaikan ucapan terima kasih kepada yang terhormat :

1) Dewan Penguji 1, Pak Hanif Al Fatta, S.Kom., M.Kom., Ph.D. dan Penguji 2, Pak Robert Marco, S.T., M.T., Ph.D yang telah memberikan saran dan masukan pada Thesis penulis.
2) Pak Alva Hendi Muhammad, S.T., M.Eng., Ph.D. selaku pembimbing atas segala arahan, masukan, motivasi, dan perhatiannya dalam membimbing penulis menyelesaikan Tesis saya, terimakasih banyak pak, semoga Allah SWT selalu melindungi beliau dan seluruh keluarganya, Aamiin.
3) Segenap dosen dan staff Program Studi Teknik Informatika Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis.
4) Pinkan Apriyana selaku support sistem saya, yang selalu mensupport dari jauh, walaupun kita berjauhan tetapi tetap didukung oleh dia, terimakasih atas dukungan nya.
5) Taufik, fajar respati, andri, reza teman-teman dari papua barat yang telah memberikan support dan semangat dari jauh kepada saya, Beno, Bagas, Aziz, Yazid, Valdo teman-teman yang berada dijojga atas dukungan, dan motivasi selama ini.
6) Teman-teman S2 saya, sadam, david, rio, deni, yusuf, arya dan teman-teman yang lain terima kasih atas supportnya.
7) Anime dan Game yang telah menemani ketika saya jenuh selama Tesis.

8) Semua pihak yang telah banyak membantu dalam penyusunan Tugas Akhir Skripsi yang tidak bisa saya sebutkan satu per satu.

Penulis menyadari masih ada banyak kekurangan dalam penyusunan Tesis ini, untuk itu penulis mengharapkan saran dan masukan untuk perbaikan. Semoga segala bantuan yang telah diberikan dari semua pihak diatas menjadi amalan yang bermanfaat baik bagi pembaca atau pihak yang membutuhkan.

Wassalamualaikum Warahmatullahi Wabarakatuh

Yogyakarta, 3 Oktober 2025

Fajar Maulana Ahsan Abbas

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Ketergantungan institusi pemerintah terhadap Teknologi Informasi (TI) untuk mendukung operasionalnya membawa serta risiko yang perlu dikelola secara efektif. Penelitian ini bertujuan untuk mengevaluasi tingkat kapabilitas manajemen risiko TI di Kantor DPRD Kota Sorong menggunakan kerangka kerja COBIT 2019, dengan fokus pada domain APO12 (Managed Risk).

Metode penelitian menggunakan pendekatan studi kasus kualitatif dengan teknik pengumpulan data melalui kuesioner, wawancara, dan observasi. Analisis data dilakukan dengan menghitung tingkat kapabilitas proses saat ini (as-is) dan melakukan analisis kesenjangan (gap analysis) terhadap tingkat target (to-be). Hasil penelitian menunjukkan bahwa tingkat kapabilitas domain APO12 secara keseluruhan berada pada Level 2 (Managed).

Ditemukan adanya paradoks kematangan, di mana institusi menunjukkan kapabilitas matang (Level 3) pada proses teknis seperti analisis dan respons risiko, namun sangat lemah (Level 1) pada proses fundamental yaitu pemeliharaan profil risiko (APO12.03) dan komunikasi risiko (APO12.04). Kesenjangan ini memutus siklus manajemen risiko yang efektif. Rekomendasi utama difokuskan pada implementasi Risk Register terpusat dan Standar Operasional Prosedur (SOP) Komunikasi Risiko untuk mengintegrasikan siklus tersebut, sehingga dapat meningkatkan kematangan tata kelola dan mendukung pencapaian tujuan strategis institusi.

Kata kunci: Tata Kelola TI, Manajemen Risiko, COBIT 2019, Audit TI, Tingkat Kapabilitas, APO12, Sektor Publik.

ABSTRACT

The reliance of government institutions on Information Technology (IT) to support their operations brings inherent risks that must be managed effectively. This research aims to evaluate the capability level of IT risk management at the Sorong City DPRD Office using the COBIT 2019 framework, focusing on the APO12 (Managed Risk) domain.

The research method employed a qualitative case study approach with data collection techniques including questionnaires, interviews, and observations. Data analysis was conducted by calculating the current process capability level (as-is) and performing a gap analysis against the target level (to-be). The results indicate that the overall capability level of the APO12 domain is at Level 2 (Managed).

A maturity paradox was identified, where the institution demonstrates mature capabilities (Level 3) in technical processes such as risk analysis and response, yet is significantly weak (Level 1) in fundamental processes, namely maintaining a risk profile (APO12.03) and articulating risk (APO12.04). This gap disconnects the effective risk management cycle. The primary recommendations focus on the implementation of a centralized Risk Register and a Standard Operating Procedure (SOP) for Risk Communication to integrate the cycle, thereby enhancing governance maturity and supporting the achievement of the institution's strategic objectives.

Keyword: *IT Governance, Risk Management, COBIT 2019, IT Audit, Capability Level, APO12, Public Sector.*

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dalam era transformasi digital yang berkembang pesat, teknologi informasi (TI) telah menjadi fondasi kritis bagi operasional dan strategi organisasi di berbagai sektor, termasuk pemerintahan, bisnis, dan layanan publik[1]. Institusi pemerintah, secara khusus lembaga legislatif seperti Dewan Perwakilan Rakyat Daerah (DPRD), sangat bergantung pada sistem TI untuk menunjang efektivitas dan efisiensi kegiatan administratif, komunikasi, dan pengelolaan data. Integrasi TI yang mendalam ini menjadi sebuah keniscayaan untuk mendukung fungsi-fungsi vital seperti proses legislasi, penganggaran, dan pengawasan publik, sekaligus menjawab tuntutan masyarakat akan transparansi dan akuntabilitas dalam dinamika sosial-politik yang semakin cepat[2]. Kemajuan TI tidak hanya meningkatkan efisiensi dan produktivitas, tetapi juga membawa kompleksitas baru dalam bentuk risiko siber, kerentanan sistem, ketidakpatuhan regulasi, dan potensi gangguan operasional. Organisasi yang gagal mengelola risiko ini secara proaktif dapat menghadapi dampak serius, mulai dari kerugian finansial, penurunan kepercayaan publik, hingga kegagalan dalam mencapai tujuan strategis[3].

Namun, tingginya tingkat ketergantungan pada infrastruktur digital secara simultan mengekspos organisasi pada spektrum risiko yang semakin luas dan kompleks[4]. Lembaga pemerintah merupakan target utama dari berbagai ancaman siber, mulai dari upaya peretasan untuk pencurian data sensitif, serangan

ransomware yang dapat melumpuhkan layanan, hingga risiko kehilangan data dan ketidakpatuhan terhadap regulasi yang berlaku. Kegagalan dalam mengelola risiko-risiko ini secara proaktif dapat mengakibatkan dampak serius, tidak hanya berupa kerugian finansial, tetapi juga disrupsi operasional, pelanggaran data, penurunan kepercayaan publik, dan pada akhirnya kegagalan institusi dalam mencapai tujuan strategisnya[5].

Secara spesifik, penelitian dalam bidang tata kelola TI di sektor publik seringkali berfokus pada lembaga eksekutif yang berorientasi pada layanan. Dalam studi yang secara mendalam menganalisis penerapan tata kelola TI di lembaga legislatif seperti Dewan Perwakilan Rakyat Daerah (DPRD), pengukuran tingkat kapabilitas manajemen risiko TI di lingkungan DPRD menjadi krusial karena adanya karakteristik unik yang membedakannya dengan instansi pemerintah lainnya. Berbeda dengan instansi eksekutif, DPRD memiliki tiga fungsi inti legislasi, penganggaran, dan pengawasan yang sangat bergantung pada integritas dan ketersediaan data.

Karakteristik unik tersebut antara lain:

a. Sensitivitas Data Legislatif: DPRD mengelola data yang sangat sensitif dan strategis, seperti draf rancangan peraturan daerah (Raperda), risalah rapat, dan data aspirasi publik. Kebocoran atau kehilangan data ini tidak hanya menimbulkan kerugian operasional, tetapi juga dapat berdampak pada stabilitas politik dan hukum di daerah.

b. Tingginya Tuntutan Transparansi dan Akuntabilitas: Sebagai representasi rakyat, kegagalan sistem TI, seperti website yang tidak dapat diakses, dapat secara langsung merusak citra dan kepercayaan publik.

c. Dinamika Proses Bisnis yang Tinggi: Proses legislasi dan pengawasan seringkali melibatkan kolaborasi intensif dalam waktu yang singkat, sehingga menuntut keandalan sistem TI yang tinggi.

Kantor DPRD Kota Sorong, dengan perannya yang sentral dalam pemerintahan daerah, menjalankan mandat yang sangat bergantung pada ketersediaan, integritas, dan kerahasiaan informasi yang dikelola melalui sistem TI. Meskipun TI telah menjadi bagian integral dari proses kerja sehari-hari, evaluasi yang sistematis dan menyeluruh terhadap kerangka pengelolaan risiko TI di lingkungan institusi ini belum pernah dilakukan secara formal. Sebagai objek penelitian, observasi awal mengidentifikasi adanya ketidakselarasan antara peningkatan adopsi TI dalam proses kerja sehari-hari dengan formalitas pengelolaan risikonya. Praktik manajemen risiko yang ada cenderung bersifat reaktif dan belum terstruktur yang secara eksplisit mengatur tentang manajemen risiko TI. Kesenjangan tata kelola ini menciptakan kondisi rentan di mana ancaman tidak teridentifikasi secara komprehensif, sehingga strategi mitigasi yang ada kemungkinan tidak memadai.

Oleh karena itu, pengelolaan risiko TI yang baik menjadi sangat penting agar DPRD dapat menjalankan fungsinya secara efektif, transparan, dan akuntabel. Evaluasi terhadap tata kelola risiko TI di DPRD. Untuk menjembatani kesenjangan tersebut, diperlukan sebuah kerangka kerja tata kelola yang terstruktur. Framework

COBIT 2019 hadir sebagai solusi yang relevan untuk meningkatkan tata kelola TI di sektor pemerintahan, dari 40 domain dalam COBIT 2019, penelitian ini hanya berfokus pada domain APO12 (*Managed Risk*) dari kelompok domain APO (*Align, Plan, and Organise*). Keputusan ini didasarkan pada argumentasi bahwa manajemen risiko merupakan fondasi tata kelola yang paling fundamental. Sebelum mengevaluasi domain lain yang berfokus pada layanan (DSS) atau optimalisasi (BAI), adalah krusial untuk memastikan bahwa institusi memiliki kapabilitas untuk melindungi aset dan menjamin keberlangsungan operasionalnya. Mengingat kondisi eksisting di objek penelitian yang menunjukkan kelemahan pada aspek ini, maka evaluasi terhadap domain APO12 (*Managed Risk*) menjadi prioritas strategis yang paling utama termasuk lembaga legislatif. Kerangka ini menyediakan pedoman komprehensif untuk menilai dan meningkatkan kapabilitas tata kelola TI, sekaligus memastikan bahwa strategi teknologi informasi sejalan dengan tujuan organisasi[6].

Domain APO12 (*Managed Risk*) dipilih sebagai fokus utama penelitian karena relevansinya yang tinggi dengan tantangan yang dihadapi Kantor DPRD Kota Sorong. Sebagai lembaga publik yang semakin bergantung pada aset informasi digital, institusi ini menghadapi peningkatan risiko siber, operasional, dan kepatuhan. Mengelola risiko-risiko ini secara efektif adalah prasyarat fundamental untuk menjamin integritas data legislatif, kelancaran layanan administrasi, dan menjaga kepercayaan publik. Oleh karena itu, evaluasi mendalam pada domain APO12 memiliki urgensi tertinggi dibandingkan domain lain untuk memastikan fondasi tata kelola TI yang aman dan andal[7].

APO12 bertujuan untuk memastikan proses manajemen risiko TI yang berkesinambungan, mencakup identifikasi, penilaian, dan mitigasi risiko yang berhubungan dengan sistem teknologi informasi[8]. Selain itu, APO12 juga mendorong integrasi pengelolaan risiko TI ke dalam kerangka manajemen risiko organisasi secara menyeluruh, sehingga selaras dengan tujuan strategis Kantor DPRD Kota Sorong. Dengan penerapan yang tepat, pendekatan ini diharapkan dapat menghasilkan rekomendasi yang efektif untuk memperkuat tata kelola risiko TI, sehingga mendukung terciptanya pelayanan publik yang aman, transparan, dan akuntabel.

Penelitian ini bertujuan untuk mengevaluasi tingkat kapabilitas pengelolaan risiko teknologi informasi di Kantor DPRD Kota Sorong berdasarkan panduan dari domain APO12 COBIT 2019. Secara mendalam, penelitian ini akan mengidentifikasi kesenjangan (*gap*) antara tingkat kapabilitas saat ini dengan tingkat yang diharapkan, serta merumuskan rekomendasi strategis yang terukur dan aplikatif untuk peningkatan di masa mendatang. Hasil penelitian diharapkan dapat memberikan kontribusi praktis dalam bentuk penguatan ketahanan operasional dan keamanan informasi bagi Kantor DPRD Kota Sorong, sekaligus memberikan kontribusi teoretis sebagai referensi empiris bagi institusi sejenis dalam menerapkan kerangka kerja COBIT 2019 untuk pengelolaan risiko TI yang lebih efektif dan akuntabel.

1.2 Rumusan Masalah

a) Bagaimana hasil evaluasi tingkat kapabilitas (*capability level*) pada setiap praktik manajemen dalam domain APO12 (*Managed Risk*) di Kantor DPRD Kota Sorong?

b) Bagaimana analisis terhadap pola sebaran kapabilitas yang ada, khususnya dalam mengidentifikasi adanya kesenjangan (*gap*) dan fenomena paradoks kematangan antara proses fundamental dengan proses teknis?

c) Rekomendasi strategis apa yang dapat dirumuskan untuk mengatasi akar permasalahan yang teridentifikasi dan membentuk siklus manajemen risiko yang utuh dan terintegrasi?

1.3 Batasan Masalah

a) Penelitian ini hanya dilakukan pada ruang lingkup Kantor DPRD Kota Sorong.

b) Untuk evaluasi, kerangka kerja COBIT 2019 akan digunakan, terutama pada domain APO12 (Manage Risk) yang berfokus pada Manajemen Risiko TI.

c) Sumber data penelitian akan diperoleh melalui observasi, dokumentasi, penyebaran kuesioner, dan wawancara dengan pihak terkait di Kantor DPRD Kota Sorong, untuk menilai kapabilitas pengelolaan risiko TI sesuai subdomain APO12.

d) Penelitian ini berfokus pada tata kelola manajemen risiko TI di Kantor DPRD Kota Sorong, dengan penekanan pada domain APO12 (*Manage Risk*) dari COBIT 2019.

e) Penelitian ini merupakan sebuah kegiatan evaluasi (audit) yang output-nya berhenti pada tahap perumusan rekomendasi dan peta jalan (*roadmap*) implementasi. Penelitian ini tidak mencakup tahap implementasi atau pengujian dari rekomendasi yang diusulkan.

f) Penelitian ini hanaya menggunakan COBIT 2019 sebagai standar audit.

1.4 Tujuan Penelitian

a) Mengukur tingkat kapabilitas pengelolaan risiko TI di Kantor DPRD Kota Sorong menggunakan framework COBIT 2019 domain APO12.

b) Mengidentifikasi kesenjangan antara kondisi aktual dan target tingkat kapabilitas yang diharapkan.

c) Memberikan rekomendasi perbaikan yang strategis dan aplikatif untuk meningkatkan pengelolaan risiko TI di Kantor DPRD Kota Sorong.

1.5 Manfaat Penelitian

a) Memberikan pemahaman mengenai IT Audit yang berfokus pada manajemen risiko di sistem teknologi informasi Kantor DPRD Kota Sorong.

b) Memberikan rekomendasi teknis bagi Kantor DPRD Kota Sorong untuk melaksanakan evaluasi sebagai langkah penanggulangan terhadap risiko yang sedang dihadapi maupun potensi risiko di masa mendatang.

BAB 2

TINJAUAN PUSTAKA

2.1 Tijauan Pustaka

Penelitian pertama berjudul "*IT Governance Maturity Assessment at PT PLN Suluttenggo Using COBIT 2019*" menekankan peran penting tata kelola teknologi informasi dalam meningkatkan efisiensi operasional, meminimalkan risiko, serta memastikan keselarasan antara strategi TI dan tujuan bisnis. Dalam studi ini, kerangka kerja COBIT 2019 dimanfaatkan dengan fokus pada Design Factors dan Governance Objectives untuk mengukur tingkat kematangan tata kelola TI. Pengumpulan data dilakukan melalui wawancara terstruktur menggunakan COBIT 2019 Design Toolkit serta analisis terhadap sepuluh faktor desain utama. Hasil penelitian mengungkap adanya kesenjangan pada beberapa proses tata kelola, khususnya pada domain APO12 (Managed Risk) yang memerlukan peningkatan signifikan demi menjamin kelancaran operasional dan pengelolaan risiko yang optimal. Rekomendasi strategis yang dihasilkan membuktikan bahwa COBIT 2019 efektif digunakan sebagai instrumen evaluasi dan perbaikan tata kelola TI pada organisasi berskala besar di sektor strategis[9].

Penelitian kedua berjudul "*Information Technology Governance Design in Trading Companies Using the COBIT 2019 Framework*" membahas peran krusial tata kelola teknologi informasi dalam mendukung pencapaian tujuan strategis organisasi, mengurangi risiko, dan mengoptimalkan penggunaan sumber daya. Studi ini menerapkan kerangka kerja COBIT 2019 untuk merancang model tata

kelola TI yang sesuai dengan karakteristik perusahaan dagang, dengan penekanan pada keamanan informasi, keselarasan TI dengan arah strategis bisnis, serta pemenuhan persyaratan kepatuhan. Pendekatan penelitian yang digunakan adalah studi kasus dengan metode kualitatif dan kuantitatif melalui observasi, wawancara, telaah pustaka, survei, dan kuesioner. Hasil pengumpulan data dianalisis menggunakan pengukuran tingkat kapabilitas serta analisis kesenjangan, yang kemudian menjadi dasar penyusunan rekomendasi perbaikan tata kelola TI[10].

Penelitian ketiga berjudul "*Information System Governance Evaluation at Diskominfo Central Java Using COBIT 2019 Framework*" membahas urgensi penilaian tata kelola sistem informasi pada lembaga pemerintah untuk memperoleh gambaran komprehensif terkait tingkat kapabilitas yang sudah dicapai. Penelitian ini menerapkan kerangka kerja COBIT 2019 yang dikombinasikan dengan CMMI sebagai acuan evaluasi, dengan pemilihan responden berdasarkan model RACI untuk menjaga keakuratan data. Proses penelitian melibatkan wawancara, pengisian kuesioner, observasi, serta penelaahan dokumen, yang kemudian dianalisis menggunakan pemetaan design factors dan analisis kesenjangan pada domain yang relevan. Temuan penelitian menunjukkan bahwa beberapa domain telah mencapai target yang diharapkan, sementara sebagian lainnya masih memerlukan perbaikan, khususnya pada aspek keamanan layanan dan pengendalian proses bisnis. Hasil ini menegaskan bahwa penggunaan COBIT 2019 dapat mendukung instansi pemerintah dalam memperkuat tata kelola TI yang adaptif, transparan, serta dapat menjadi acuan bagi pengembangan layanan publik digital di wilayah lain[11].

Penelitian keempat berjudul "Evaluasi Tata Kelola Teknologi Informasi Pada PT Indako Trading Coy Dengan Menggunakan Framework COBIT 2019 Domain APO12" bertujuan menilai tingkat kapabilitas tata kelola TI perusahaan dengan fokus pada pengelolaan risiko. Kerangka kerja COBIT 2019, khususnya domain APO12 (*Manage Risk*), digunakan sebagai acuan untuk mengidentifikasi kesenjangan antara kondisi tata kelola yang ada dengan standar yang diharapkan. Metode penelitian meliputi wawancara, kuesioner, dan analisis dokumen, yang menghasilkan temuan bahwa tingkat kapabilitas perusahaan berada pada level yang memerlukan peningkatan, terutama dalam aspek identifikasi, penilaian, dan mitigasi risiko TI. Hasil penelitian memberikan rekomendasi strategis agar pengelolaan risiko TI dapat lebih efektif, terukur, dan selaras dengan tujuan bisnis perusahaan[12].

Penelitian kelima berjudul "Audit Manajemen Masalah Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019 Domain DSS03" membahas evaluasi pengelolaan masalah dalam layanan TI untuk memastikan proses penanganan insiden dan masalah berjalan efektif serta mendukung keberlangsungan operasional organisasi. Kerangka kerja COBIT 2019 digunakan sebagai acuan, dengan fokus pada domain DSS03 (*Manage Problems*), guna menilai sejauh mana tingkat kapabilitas proses yang telah diterapkan. Pengumpulan data dilakukan melalui wawancara, kuesioner, observasi, dan studi dokumen. Hasil analisis menunjukkan adanya kesenjangan antara kondisi aktual dengan target kapabilitas yang diharapkan, khususnya dalam dokumentasi masalah, analisis akar penyebab, dan penerapan solusi permanen. Penelitian ini memberikan rekomendasi

perbaikan yang diharapkan dapat meningkatkan efektivitas manajemen masalah TI serta mendukung pencapaian tujuan organisasi[13].

Penelitian terakhir berjudul "Audit Tata Kelola TI Menggunakan COBIT 2019 Domain APO12 Pada Universitas Mikroskil" bertujuan mengevaluasi tingkat kapabilitas manajemen risiko TI di lingkungan perguruan tinggi menggunakan kerangka kerja COBIT 2019, khususnya domain APO12 (*Manage Risk*). Data penelitian dikumpulkan melalui kuesioner, wawancara, dan studi dokumen, kemudian dianalisis untuk mengidentifikasi kesenjangan antara kondisi tata kelola saat ini dengan standar yang direkomendasikan COBIT 2019. Hasil penelitian menunjukkan bahwa tingkat kapabilitas berada di bawah target yang diharapkan, dengan kelemahan utama pada proses identifikasi dan mitigasi risiko. Penelitian ini memberikan rekomendasi perbaikan yang difokuskan pada peningkatan prosedur pengelolaan risiko agar lebih efektif, terdokumentasi, dan selaras dengan tujuan strategis organisasi[14].

2.2 Keaslian Penelitian

Tabel 2.1 Matriks literatur review dan posisi penelitian

Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: Kantor DPRD Kota Sorong)

No	Judul Penelitian	Nama Peneliti, Tahun, Index	Metode Penelitian	Hasil	Keunggulan dan Kelemahan	Perbandingan
1	*IT Governance Maturity Assessment at PT PLN Suluttengo Using COBIT 2019*	George Morris William Tangka, Cherry Luningkewas, Ericnika Lompoliu, 2025, Sinta 4	Evaluasi kematangan tata kelola TI menggunakan COBIT 2019 (Multi-domain). Fokus pada *Design Factors* dan *Governance Objectives*. Data dikumpulkan melalui wawancara terstruktur menggunakan COBIT 2019 Design Toolkit	Mengidentifikasi berbagai level kapabilitas (Level 1-5) di berbagai d Secara spesifik menyoroti Manajemen Risiko TI (APO12) sebagai salah satu area tantangan yang memerlukan perbaikanomain.	**Keunggulan:** Menggunakan *Design Toolkit* COBIT 2019 untuk memprioritaskan domain audit. **Kelemahan :** Tantangan pada manajemen risiko TI, eksekusi proyek, dan optimalisasi investasi TI.	Penelitian ini mengevaluasi banyak domain COBIT 2019 secara umum, sedangkan penelitian saya fokus pada domain APO12 untuk memetakan dan memperbaiki manajemen risiko TI di Kantor DPRD Kota Sorong.
2	*Information Technology Governance Design in Trading Company*	Kevin Leonardo, Rudi Latuperissa, 2024, Q3	Perancangan tata kelola TI (COBIT 2019 Multi-domain). Menggunakan studi	Menghasilkan desain tata kelola yang disesuaikan kebutuhan.	**Keunggulan:** Fokus pada perancangan sistem tata kelola dari	Penelitian ini fokus pada desain tata kelola TI, sedangkan penelitian saya fokus pada evaluasi

	Using COBIT 2019 Framework		kasus kualitatif & kuantitatif (Observasi, Wawancara, Kuesioner). Melibatkan analisis *Design Factors*	Penelitian ini tidak melakukan evaluasi kapabilitas, melainkan merancang dari awal	awal sesuai kebutuhan bisnis. **Kelemahan:** Sistem TI tidak terintegrasi, kerentanan keamanan data, dan kapabilitas karyawan yang tidak memadai	kapabilitas pengelolaan risiko TI.
3	*Information System Governance Evaluation at Diskominfo Central Java Using COBIT 2019 Framework*	Ahmad Zaini, Aris Puji Widodo, Dinar Mutiara Kusumo Nugraheni, 2025, Sinta 2	Evaluasi tata kelola SI menggunakan COBIT 2019 Domain DSS01-DSS06. Mengkombinasikan COBIT 2019 dengan CMMI. Menggunakan triangulasi data untuk validitas	Sebagian besar domain telah mencapai target (Level 4 atau 5). Namun, ditemukan *gap* pada DSS03, DSS05, dan DSS06 yang masih di Level 3 (target Level 4)	**Keunggulan:** Menggunakan triangulasi data untuk validitas. *Novelty* pada integrasi COBIT 2019 & CMMI **Kelemahan:** Perlu perbaikan pada keamanan layanan (*security services*) dan kontrol proses bisnis	Penelitian ini serupa dalam menggunakan COBIT 2019, namun fokus domain berbeda. Penelitian saya akan fokus pada APO12 di Kantor DPRD Kota Sorong yang berhubungan dengan manajemen risiko.
4	Evaluasi Tata Kelola Teknologi Informasi pada PT Indako	Stanley Howard, Tomy Wijaya, Roni	Evaluasi tata kelola TI menggunakan COBIT 2019 Domain APO12.	*Capability Level* berada pada Level 2. *Maturity Level*	**Keunggulan:** Menyajikan perbandingan gap	PT Indako sektor swasta, hambatan koordinasi internal, sedangkan Kantor

	Trading Coy dengan Menggunakan Framework COBIT 2019 Domain APO12	Yunis, Megawati, 2023	Metode kualitatif, dengan pengumpulan data melalui wawancara dan kuesioner	juga berada pada Level 2 (*Managed Process*). Ditemukan *gap* 1 level dari target (Level 3)	secara visual menggunakan grafik radar. **Kelemahan:** Belum adanya manajemen risiko yang baik; dokumentasi minim dan tidak formal	DPRD Kota Sorong sektor pemerintahan, hambatan birokrasi.
5	Audit Manajemen Masalah Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019 Domain DSS03	Danu Prawira Utama, Alva Hendi Muhammad, Agus Purwanto, 2023, Sinta 2	Audit tata kelola TI menggunakan COBIT 2019 Domain DSS03 (Manage Problem). Metode eksploratif, pengumpulan data melalui studi naskah dan wawancara (kuesioner)	*Capability Level* berada pada Level 4 (*Predictable Process*). Ditemukan *gap* 1 level pada beberapa subdomain (DSS03.04 dan DSS03.05) dari target Level 5	**Keunggulan:** Mencapai level kapabilitas yang tinggi. **Kelemahan:** Masih ditemukan kekurangan dalam dokumentasi dan tindak lanjut penyelesaian masalah	Persamaan: Sama-sama menggunakan framework COBIT 2019 untuk evaluasi tata kelola TI. Perbedaan: Penelitian ini fokus pada domain DSS03 terkait manajemen masalah, sedangkan penelitian saya fokus pada domain APO12 terkait manajemen risiko TI di lembaga pemerintahan.

6	Audit Tata Kelola TI Menggunakan COBIT 2019 Domain APO12 Pada Universitas Mikroskil	Chandra Wijaya, Mario Sukamto, Roni Yunis, Megawati, 2023, Sinta 4	Audit tata kelola TI menggunakan COBIT 2019 Domain APO12. Metode kualitatif, dengan pengumpulan data melalui wawancara dan kuesioner	*Capability Level* berada pada Level 1 (*Performed*). *Maturity Level* berada pada Level 2 (*Managed*).	**Keunggulan:** Melakukan pengukuran *Capability* dan *Maturity Level* secara terpisah. **Kelemahan:** Prosedur risiko belum terdokumentasi dengan baik, menjadi kelemahan utama	Penelitian ini dilakukan di sektor pendidikan dengan fokus pada sistem akademik dan operasional kampus, sedangkan penelitian saya di DPRD Kota Sorong berfokus pada sistem informasi perkantoran dan proses birokrasi pemerintahan.

2.3 Landasan Teori

2.3.1 Kantor DPRD Kota Sorong

Gambar 2.1 Kantor DPRD Kota Sorong

Kantor Dewan Perwakilan Rakyat Daerah (DPRD) Kota Sorong merupakan lembaga legislatif yang memiliki peran penting dalam sistem pemerintahan daerah di Indonesia, khususnya di Kota Sorong, Jl. Sungai Maruni Km.10 Kota Sorong Provinsi Papua Barat Daya. Sebagai lembaga yang mewakili suara rakyat, DPRD bertugas untuk menyusun, membahas, dan menetapkan peraturan daerah, serta mengawasi pelaksanaan kebijakan pemerintah daerah. DPRD juga berfungsi sebagai jembatan antara masyarakat dan pemerintah, menampung aspirasi, serta mengadvokasi kepentingan publik dalam pengambilan keputusan yang berkaitan dengan pembangunan dan pelayanan masyarakat. DPRD Kota Sorong terdiri dari anggota yang dipilih melalui pemilihan umum, yang mewakili berbagai partai politik. Anggota DPRD memiliki masa jabatan tertentu, biasanya selama lima tahun, dan mereka bertanggung jawab untuk menjalankan fungsi legislasi,

anggaran, dan pengawasan. Dalam melaksanakan tugasnya, DPRD berkolaborasi dengan pemerintah daerah, termasuk Walikota dan perangkat daerah lainnya, untuk memastikan bahwa kebijakan yang diambil sesuai dengan kebutuhan dan harapan masyarakat.

2.3.2 Audit

Audit adalah suatu proses pemeriksaan yang dilakukan secara independen untuk menilai sejauh mana suatu organisasi atau sistem telah berjalan sesuai dengan ketentuan, prosedur, dan standar yang berlaku. Proses ini mencakup kegiatan pengumpulan, pengujian, dan evaluasi bukti secara sistematis untuk memastikan bahwa informasi yang disampaikan oleh suatu entitas benar, akurat, dan dapat dipercaya. Audit tidak hanya berfokus pada keakuratan data, tetapi juga menilai tingkat kepatuhan terhadap regulasi, efektivitas pelaksanaan prosedur, serta efisiensi penggunaan sumber daya. Tujuan utama dari pelaksanaan audit adalah memberikan keyakinan dan jaminan kepada para pemangku kepentingan bahwa sistem, proses, atau laporan yang diaudit telah memenuhi persyaratan dan standar yang ditetapkan, sehingga dapat dijadikan dasar dalam pengambilan keputusan yang tepat[15].

2.3.3 Pelaksanaan Audit

Audit sistem informasi merupakan proses independen yang bertujuan mengumpulkan dan mengevaluasi bukti untuk memastikan bahwa sistem informasi suatu organisasi mampu melindungi aset, menjaga integritas data, serta beroperasi secara optimal dalam mencapai tujuan organisasi. Cakupan audit ini meliputi aspek keamanan informasi, pengendalian internal, dan kepatuhan terhadap kebijakan

maupun peraturan yang berlaku. Hasil audit diharapkan dapat memberikan penilaian yang objektif mengenai tingkat keandalan sistem informasi dan kesesuaiannya dengan standar yang telah ditetapkan.

Pelaksanaan audit sistem informasi melibatkan pengumpulan serta analisis data yang berkaitan dengan penggunaan dan pengelolaan sistem, seperti informasi tentang pengguna dan sistem, contoh masukan dan keluaran, serta dokumentasi kontrol yang ada. Weber (1999) mengemukakan tiga teknik utama untuk memperoleh bukti audit, yaitu :

a. Wawancara dengan pihak terkait seperti analis sistem, pemrogram, staf operasional, pengguna, dan pengendali organisasi untuk memahami struktur kontrol, menilai risiko, serta memverifikasi penerapan kontrol input.
b. Kuesioner yang digunakan untuk menilai keberadaan, efektivitas, atau kelemahan kontrol, sekaligus mengidentifikasi potensi ketidakefisienan sistem berdasarkan persepsi pengguna.
c. Diagram alir kontrol yang memvisualisasikan letak dan jenis kontrol dalam sistem, meskipun pembuatan dan pemeliharaannya memerlukan waktu dan usaha yang cukup besar.

Seperti audit lainnya, audit sistem informasi memiliki tujuan utama memastikan efektivitas pengendalian dan kepatuhan, namun memerlukan pengetahuan teknis khusus terkait teknologi informasi. Champlain (2003) menjelaskan bahwa audit dilakukan dengan mengikuti metode standar yang berfungsi sebagai kerangka kerja bagi auditor, berisi daftar pengujian untuk

memastikan kontrol berfungsi sebagaimana mestinya. Beberapa metode audit yang dikenal luas antara lain COSO, CoCo, Cadbury, COBIT, SAC, eSAC, serta SASs, yang masing-masing digunakan baik untuk standar nasional maupun internasional.

2.3.4 Tata Kelola Teknologi Informasi

Tata kelola TI adalah suatu kerangka kerja yang memastikan penggunaan teknologi informasi dalam organisasi selaras dengan tujuan dan strategi bisnis secara keseluruhan. Tata kelola TI mencakup proses pengambilan keputusan, kebijakan, dan prosedur yang menjamin TI dimanfaatkan secara efektif untuk memberikan nilai tambah bagi organisasi sekaligus mengelola risiko yang terkait dengan penggunaannyaDalam konteks penelitian ini, tata kelola TI menjadi aspek penting dalam audit, karena merupakan bagian dari strategi TI yang berfokus pada pengelolaan instansi atau perusahaan guna menyelaraskan tujuan bisnis dengan strategi TI untuk menghasilkan nilai bisnis yang optimal[14]. Tata kelola TI juga dapat mencakup detail dari sistem yang ada serta melibatkan seluruh pemangku kepentingan dalam organisasi. Tata kelola TI memiliki tujuan utama untuk mengendalikan pemanfaatannya, sehingga kinerja yang dihasilkan memenuhi standar yang berlaku dan selaras dengan sasaran strategis organisasi. Dalam pelaksanaannya, tata kelola TI diarahkan untuk:

1. Menyelaraskan penerapan teknologi informasi dengan strategi organisasi serta memastikan realisasi manfaat yang telah dijanjikan dari implementasi TI.

2. Memanfaatkan teknologi informasi secara optimal untuk membuka dan mengelola peluang yang ada, sehingga mampu memaksimalkan keuntungan yang diperoleh.
3. Memastikan akuntabilitas dalam penggunaan sumber daya TI.
4. Mengelola risiko-risiko yang berkaitan dengan teknologi informasi secara tepat dan efektif.

Dalam tata kelola teknologi informasi (TI) terdapat empat tujuan pokok (*objectives*) yang menjadi arah sekaligus acuan dalam pengelolaannya, yaitu:

1. *Accountability* atau akuntabilitas, yang menekankan pentingnya pertanggungjawaban dalam setiap penggunaan dan pengambilan keputusan terkait TI.
2. *IT Value and Alignment*, yakni penciptaan nilai tambah melalui keselarasan antara strategi TI dengan strategi bisnis organisasi.
3. *Risk Management* atau manajemen risiko, yang berfokus pada pengendalian dan mitigasi risiko yang terkait dengan penerapan TI
4. *Performance Measurement* atau pengukuran kinerja, yang digunakan untuk menilai efektivitas dan efisiensi pemanfaatan TI.

Secara umum, tata kelola TI bertujuan untuk memastikan bahwa informasi yang dihasilkan dapat dipertanggungjawabkan, sekaligus memberikan nilai tambah bagi proses bisnis yang dijalankan oleh organisasi. Di samping itu, tata kelola TI berperan dalam meminimalkan risiko yang berkaitan dengan pemanfaatan TI, serta menyediakan kerangka evaluasi untuk mengukur kinerja dari implementasi TI tersebut[16].

2.3.5 Risiko

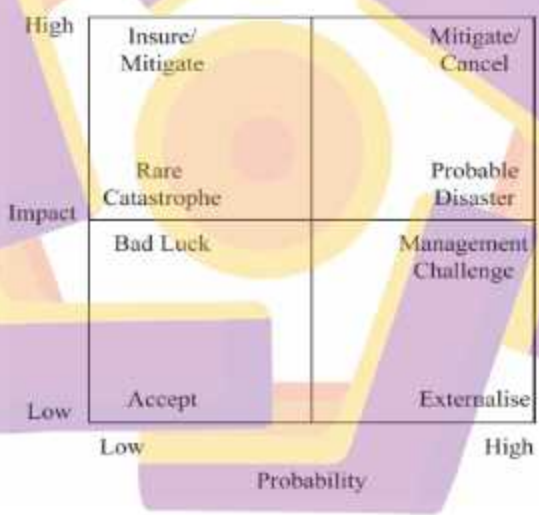
Konsep risiko dapat dipahami melalui berbagai perspektif, mulai dari definisi leksikal hingga kerangka kerja teknis dalam tata kelola organisasi. Secara leksikal, Kamus Besar Bahasa Indonesia (KBBI) mendefinisikan risiko sebagai suatu akibat yang bersifat kurang menyenangkan, merugikan, atau membahayakan. Dalam lingkup tata kelola organisasi yang lebih spesifik, risiko dipandang sebagai faktor yang secara langsung memengaruhi pencapaian target. Menurut Keputusan Menteri Keuangan (KMK) Nomor 577/KMK.01/2019, risiko merupakan kemungkinan terjadinya sebuah peristiwa yang berdampak terhadap pencapaian sasaran organisasi. Dampak yang ditimbulkan cenderung negatif dan dalam skenario terburuk dapat mengancam keberlangsungan hidup organisasi itu sendiri[17].

Pandangan ini selaras dengan standar internasional ISO 31000 (melalui ISO Guide 73), yang merumuskan risiko secara presisi sebagai "pengaruh dari ketidakpastian terhadap tujuan" yang ingin dicapai. Dari berbagai definisi tersebut, dapat disintesiskan bahwa elemen-elemen fundamental dari risiko mencakup adanya ketidakpastian (*uncertainty*), potensi suatu peristiwa (*event*), dan dampak (*impact*) dari peristiwa tersebut terhadap pencapaian tujuan (*objectives*) yang telah ditetapkan oleh sebuah entitas atau organisasi[7].

2.3.6 Klasifikasi Risiko

Risiko dalam suatu proses dapat dibedakan berdasarkan sifatnya yang berkaitan dengan kegiatan bisnis maupun non-bisnis. Secara umum, terdapat dua bentuk risiko dasar, yaitu *speculative risk dan pure risk*. *Speculative risk* adalah

jenis risiko yang mengandung kemungkinan terjadinya keuntungan maupun kerugian, sehingga hasil yang diperoleh dapat bernilai positif atau negatif. Sementara itu, *pure risk* merupakan jenis risiko yang hanya menimbulkan dua kemungkinan, yaitu kerugian atau tidak mengalami kerugian sama sekali, tanpa adanya peluang untuk memperoleh keuntungan[18]. Menurut National Academy of Sciences (2005), terdapat pula konsep risiko yang menguraikan tingkatannya, yang berfungsi sebagai kerangka untuk mengidentifikasi, menilai, dan mengelola risiko sesuai dengan potensi dampaknya terhadap organisasi.



Gambar 2.1 *Risk Impacts and Probability Matrix*

Berdasarkan Gambar 2.2 mengenai *Risk Impacts and Probability Matrix*, terdapat empat kategori risiko yang dikelompokkan berdasarkan kombinasi tingkat dampak (*impact*) dan kemungkinan terjadinya (*probability*), yaitu:

a) *Low Impact – Low Probability*

Kategori ini menggambarkan risiko dengan tingkat dampak dan probabilitas yang rendah. Pada konteks risiko negatif, kategori ini umumnya tidak memerlukan respons manajerial yang bersifat proaktif, karena ancamannya relatif kecil dan kemungkinan terjadinya jarang.

b) *High Impact – Low Probability*

Risiko pada kategori ini memiliki dampak yang signifikan, namun probabilitas terjadinya rendah. Tingkat risikonya dapat berkisar dari rendah hingga tinggi, namun umumnya dikategorikan sebagai risiko tingkat sedang, bergantung pada ambang batas yang ditetapkan organisasi. Peristiwa pada kategori ini biasanya jarang terjadi dan dapat diklasifikasikan sebagai bencana langka, sehingga sulit memperkirakan probabilitasnya akibat keterbatasan data historis.

c) *Low Impact – High Probability*

Kategori ini mencakup risiko yang memiliki dampak rendah tetapi probabilitas terjadinya tinggi. Meskipun secara individual dampaknya kecil, akumulasi dari beberapa risiko serupa dapat meningkatkan tingkat risiko secara keseluruhan. Kategori ini umumnya berada pada tingkat risiko sedang, dengan penentuan karakteristiknya tetap mengacu pada ambang batas yang telah ditentukan organisasi.

d) *High Impact – High Probability*

Kategori ini mencerminkan risiko dengan tingkat dampak dan probabilitas yang sama-sama tinggi. Risiko negatif dalam kategori ini dapat menjadi ancaman serius terhadap pencapaian tujuan organisasi,

sehingga memerlukan penanganan prioritas dan strategi respons yang agresif. Tindakan mitigasi yang mungkin dilakukan mencakup pengurangan tingkat risiko atau bahkan penghentian proyek apabila risiko dinilai terlalu besar untuk ditangani.

2.3.7 Manajemen Risiko

Manajemen risiko muncul sebagai suatu pendekatan yang dirancang untuk memenuhi kebutuhan pengelolaan risiko secara sistematis pada sistem yang dimiliki oleh perusahaan atau instansi. Dalam konteks penerapannya, organisasi perlu memiliki kemampuan untuk mengurangi potensi risiko yang berkaitan dengan implementasi teknologi informasi (TI) maupun tata kelola TI. Kemampuan ini menjadi dasar dalam perumusan strategi penerapan TI yang tepat, efektif, dan sejalan dengan arah kebijakan organisasi. Pada praktiknya, proses manajemen risiko seringkali dijabarkan melalui penerapan standar atau kerangka kerja konvensional yang berbentuk siklus berulang, sebagaimana tergambarkan pada Gambar 2.3 yang menjelaskan Siklus ini berfungsi sebagai panduan bagi organisasi dalam melakukan identifikasi, analisis, mitigasi, serta evaluasi risiko secara berkelanjutan guna memastikan keberlangsungan dan keberhasilan implementasi TI[19].

Gambar 2.2 Siklus Manajemen Risiko

Dalam melakukan analisis terhadap risiko yang terdapat pada suatu perusahaan atau instansi, langkah awal yang perlu dilakukan adalah mengidentifikasi potensi risiko yang mungkin terjadi. Setelah proses identifikasi, tahap selanjutnya adalah melakukan penilaian terhadap tingkat risiko tersebut untuk menentukan tingkat urgensi dan dampaknya terhadap organisasi. Hasil penilaian ini kemudian dijadikan sebagai acuan dalam merumuskan langkah strategis dan tindakan mitigasi yang bertujuan meminimalkan risiko yang ada. Setelah strategi diimplementasikan dan sistem berjalan, diperlukan proses pengawasan secara berkelanjutan untuk memantau perkembangan serta mengevaluasi efektivitas langkah yang telah diterapkan. Evaluasi ini bertujuan untuk menilai sejauh mana risiko tersebut dapat dikelola atau dikurangi secara optimal, sehingga mendukung tercapainya tujuan organisasi[8], [18].

2.3.8 Proses Manajemen Risiko

Proses manajemen risiko mencakup penerapan langkah-langkah secara sistematis dan terorganisir untuk mengidentifikasi, menganalisis, serta mengendalikan potensi risiko yang dapat memengaruhi pencapaian tujuan organisasi. Dalam pelaksanaannya, manajemen risiko terdiri atas sejumlah prosedur yang saling terintegrasi, yang berfungsi sebagai panduan dalam pengelolaan risiko secara efektif dan berkelanjutan. Adapun prosedur tersebut meliputi tahapan-tahapan sebagai berikut:

Gambar 2.3 Prosedur Manajemen Risiko

Menurut ISO 31000:2009, proses manajemen risiko terdiri atas beberapa tahapan utama, yaitu *risk identification, risk analysis, risk evaluation,* dan *risk treatment* (Broadleaf, 2014). Penjabaran masing-masing tahapan adalah sebagai berikut:

a) *Risk Identification*

Tahap ini berfokus pada penentuan faktor-faktor yang dapat menimbulkan risiko, mencakup aspek apa, bagaimana, dan mengapa suatu kondisi berpotensi terjadi. Proses ini dilakukan secara komprehensif dan terstruktur dengan tujuan agar risiko dapat dikenali secara menyeluruh sehingga memudahkan penilaian pada tahap selanjutnya.

b) *Risk Analysis*

Tahap ini melibatkan analisis mendalam terhadap hasil identifikasi risiko sebelumnya. Analisis dilakukan untuk memahami sifat, penyebab, serta potensi dampak dari risiko tersebut, sehingga dapat diperoleh gambaran yang jelas mengenai tingkat keparahan dan kemungkinan terjadinya.

c) *Risk Assessment*

Pada tahap ini, fokus diarahkan pada penentuan frekuensi atau probabilitas terjadinya risiko serta besaran dampak yang mungkin ditimbulkannya. Informasi ini menjadi dasar dalam mengkategorikan risiko berdasarkan tingkat prioritas penanganan.

d) *Risk Evaluation*

Tahap evaluasi risiko dilakukan dengan membandingkan hasil perkiraan risiko terhadap kriteria atau standar risiko yang telah ditetapkan organisasi. Tujuannya adalah menentukan signifikansi risiko serta

memutuskan apakah risiko tersebut dapat diterima atau memerlukan penanganan lebih lanjut.

e) *Risk Treatment*

Tahap ini mencakup penentuan strategi dan tindakan yang akan diterapkan untuk mengendalikan atau mengurangi risiko. Pendekatan yang digunakan dapat berupa mitigasi, pencegahan, pemindahan, atau penerimaan risiko, baik terhadap risiko yang ada saat ini maupun risiko potensial di masa mendatang.

2.3.9 COBIT 2019

Menurut ISACA, 2019[19] *Control Objectives for Information and Related Technology* (COBIT) pertama kali dikeluarkan oleh Foundation for Information Systems Audit and Control pada tahun 1996, dan kemudian diperbarui pada tahun 1998 dan 2000. COBIT adalah framework yang mencakup berbagai masalah kontrol internal, terutama yang berkaitan dengan TI. Tujuan COBIT adalah untuk meneliti, mengembangkan, memperkenalkan, dan mengajukan sebuah kewenangan kontrol objektif yang modern dan dapat diterima secara internasional untuk digunakan oleh manajer bisnis dan auditor setiap hari.

Bagi beberapa organisasi, aset yang paling berharga adalah data dan teknologi pendukung. Akibatnya, COBIT menjelaskan mengapa pengaturan TI (*IT Governance*) harus dilakukan. Ini disebabkan oleh fakta bahwa ada peningkatan temuan tentang gangguan sistem informasi dan penipuan elektronik. Oleh karena itu, pengelolaan risiko TI telah dianggap sebagai bagian penting dari manajemen organisasi. Dalam framework COBIT terdapat empat domain IT, yang mencakup

empat puluh tujuan pengelolaan dan pengelolaan proses IT dan juga tujuan kontrol yang dikelompokkan ke dalam empat proses khusus IT, yaitu plan and organize, acquire and implement, deliver and support, serta monitor dan evaluasi. Saat ini, ada berbagai versi COBIT, yang paling baru adalah COBIT 2019[20].

Untuk saat ini, proses penyelarasan COBIT 2019 didasarkan pada standar framework lain, seperti ITIL (*IT Infrastructure Library*), COSO (*Komite Sponsoring Organizations of the Treadway Commission*), ISO 27001/2, dan PMBOK (*Project Management Book of Knowledge*)[20]. Dalam COBIT 2019, ada subpoint yang membahas kepatuhan (*compliance*), masalah teknik (*technical issues*), persyaratan kontrol (*control requirements*), dan risiko bisnis. Saat ini, COBIT 2019 telah banyak digunakan karena memiliki banyak kelebihan. Berikut adalah beberapa kelebihan COBIT 2019 dibandingkan dengan versi sebelumnya, yaitu :

1. Flexibel Pada COBIT 2019, Anda dapat menambah area fokus baru ataumengubah area fokus yang sudah ada, tanpa berdampak langsung pada strukturdan konten model inti.
2. Pada COBIT 2019, struktur manajemen kinerja dapat dimasukkan ke dalam model konseptual untuk membuat proses manajemen kinerja IT lebih mudahdan lebih baik.
3. Aplikasi preskriptif dapat disesuaikan dengan karakteristik model deskriptifdan preskriptif dalam COBIT 2019.
4. Relevansi, pada COBIT 2019, mendukung referensi konseptual dari berbagaisumber.

Sebagai contoh, COBIT 2019 mengalami beberapa perubahan dan penyesuaian, di antaranya:

1. COBIT 2019 membawa ide baru dan definisi terminologi. Dalam model inti COBIT, ada empat puluh tujuan pengelolaan dan manajemen yang digabungkan ke dalam platform, yang dimaksudkan untuk membantu mengarahkan pengelolaan tata kelola IT.
2. Kinerja manajemen sistem telah diperbarui, yang memungkinkan fleksibilitas dalam melakukan pengukuran tingkat kematangan dan kemampuan.
3. Untuk membuat adopsi COBIT 2019 lebih mudah untuk proyek tertentu maupun implementasi penuh, ada petunjuk tambahan di bagian introduksi faktor desain dan fokus area.

Dalam kerangka kerja COBIT, lima kategori sumber daya teknologi informasi ditunjukkan, antara lain:

a) Data adalah objek yang memiliki banyak pengertian, baik internal maupun eksternal, terstruktur maupun tidak terstruktur, berbentuk suara atau grafik, dan sebagainya.
b) Sistem aplikasi, dipahami sebagai sejumlah petunjuk (manual) dan prosedur terprogram.
c) Teknologi, Ini mencakup hardware, sistem operasi, networking, multimedia, sistem pengelolaan database, dan sebagainya.
d) Sumber daya yang diperlukan untuk menempatkan dan mendukung sistem informasi disebut sebagai fasilitas.

e) Manusia, yang mencakup kemampuan karyawan, pengetahuan, dan produktivitas yang diperlukan untuk merencanakan, mengatur, memperoleh, mengirimkan, mendukung, dan mengawasi sistem informasi dan pelayanannya.

2.3.10 Implementasi Road Map COBIT 2019

Gambar 2.4 Road Map COBIT 2019

Menurut COBIT 2019 Implementation Guide, proses implementasi COBIT 2019 dilakukan melalui tujuh tahapan yang membentuk suatu siklus berkesinambungan ISACA, 2019[19]. Tahapan-tahapan tersebut dapat diuraikan sebagai berikut:

a) Fase 1 – *Where Are the Drivers?*

Tahap ini bertujuan mengidentifikasi change drivers serta membangun komitmen perubahan pada tingkat manajemen eksekutif yang kemudian

dituangkan dalam kerangka business case. Change drivers merupakan peristiwa, kondisi, atau permasalahan utama, baik yang berasal dari faktor internal maupun eksternal, yang memicu kebutuhan perubahan. Faktor pendorong ini dapat berupa tren industri, pasar, atau teknologi; kelemahan kinerja; implementasi perangkat lunak; maupun tujuan strategis perusahaan. Risiko yang terkait dengan implementasi program diuraikan secara jelas dalam business case dan dikelola sepanjang siklus hidup proyek.

b) Fase 2 – *Where Are We Now?*

Pada tahap ini, tujuan yang berhubungan dengan informasi dan teknologi (I&T goals) diselaraskan dengan strategi dan profil risiko perusahaan. Proses ini melibatkan penentuan prioritas tujuan, penyelarasan sasaran, serta penetapan tujuan tata kelola dan manajemen. Panduan desain COBIT 2019 menyediakan berbagai faktor desain yang membantu proses pemilihan ini. Berdasarkan tujuan yang telah dipilih, organisasi kemudian mengidentifikasi sasaran tata kelola dan manajemen yang bersifat kritis serta proses utama yang memiliki kapabilitas memadai untuk mencapai hasil optimal. Evaluasi kemampuan dan kelemahan dilakukan melalui penilaian kapabilitas proses terhadap kondisi aktual.

c) Fase 3 – *Where Do We Want to Be?*

Tahap ini menetapkan target perbaikan yang diikuti oleh analisis kesenjangan (gap analysis) untuk mengidentifikasi solusi potensial.

Beberapa solusi yang ditemukan juga berfungsi untuk mengatasi risiko yang telah diidentifikasi. Prioritas diberikan pada proyek yang relatif mudah dilaksanakan dan diselesaikan, sementara inisiatif jangka panjang dipecah menjadi bagian-bagian yang lebih kecil agar lebih mudah dikelola.

d) Fase 4 – *What Needs to Be Done?*

Pada tahap ini, organisasi merumuskan perencanaan solusi yang realistis dan dapat diimplementasikan, dengan mendefinisikan proyek-proyek yang memiliki dukungan bisnis yang kuat dan selaras dengan business case yang telah disusun. Business case yang komprehensif membantu memastikan manfaat proyek dapat diukur dan perkembangan implementasinya dapat dipantau secara efektif.

e) Fase 5 – *How Do We Get There?*

Tahap ini berfokus pada pelaksanaan solusi yang telah dirumuskan pada fase sebelumnya. Proses implementasi dilengkapi dengan langkah-langkah operasional serta mekanisme pemantauan untuk memastikan keselarasan dengan tujuan bisnis dan pengukuran kinerja yang terukur.

f) Fase 6 – *Did We Get There?*

Tahap ini memastikan bahwa peningkatan praktik tata kelola dan manajemen yang telah diterapkan dapat bertransisi menjadi bagian dari operasi normal organisasi. Pemantauan dilakukan dengan menggunakan metrik kinerja dan indikator manfaat yang telah ditentukan pada fase sebelumnya.

g) Fase 7 – *How Do We Keep the Momentum Going?*

Fase terakhir menitikberatkan pada evaluasi menyeluruh atas keberhasilan inisiatif yang telah dilakukan, identifikasi kebutuhan tata kelola dan manajemen yang lebih lanjut, serta penguatan komitmen terhadap perbaikan berkelanjutan. Pada tahap ini, organisasi memprioritaskan peluang-peluang baru untuk meningkatkan efektivitas tata kelola sistem informasi.

2.3.11 COBIT Core Model

Adapun model inti dari COBIT yang terdapat dalam prosesnya yang dimana bertujuan untuk melakukan proses pengelolaan dan manajemen yang sistematis dari sebuah COBIT ISACA, 2019[19]. Berikut adalah Core Model COBIT 2019 pada gambar 2.6 berikut ini.

Gambar 2.5 COBIT 2019 Core Model

Dalam kerangka COBIT 2019 Core Model, keseluruhan komponen tata kelola dan manajemen teknologi informasi dikelompokkan ke dalam sejumlah domain. Setiap domain memiliki tujuan spesifik serta fungsi yang saling melengkapi dalam mendukung pencapaian sasaran organisasi. Adapun domain-domain yang tercakup dalam Core Model COBIT 2019 adalah *Governance Objective - Evaluate, Direct, Monitor* (EDM). Dalam domain ini, manajemen melakukan evaluasi opsi strategis, mengarahkan manajemen senior pada opsi strategis yang dipilih, dan memantau pencapaian strategi. Tujuan pengelolaan (*management objectives*) terdiri dari lima domain berikut:

a) EDM (*Evaluate, Direct and Monitor*)

Domain ini berfokus pada kegiatan evaluasi di area tata kelola, termasuk penilaian berbagai opsi strategis, pengambilan keputusan strategis yang tepat, serta pemantauan implementasi keputusan tersebut. Tujuannya adalah memastikan bahwa strategi yang dipilih selaras dengan tujuan organisasi dan dijalankan secara efektif.

b) APO (*Align, Plan and Organize*)

Domain ini menggambarkan aspek perencanaan dan pengorganisasian tata kelola TI, mencakup struktur organisasi, penyusunan strategi, serta pengaturan aktivitas pendukung TI secara menyeluruh. Lingkupnya mencakup pengelolaan sumber daya, kapabilitas, dan arah strategis TI agar selaras dengan tujuan bisnis.

c) BAI (*Build, Acquire and Implement*)

Domain ini mencakup proses perancangan, pengadaan, serta implementasi solusi teknologi informasi, termasuk integrasinya ke dalam proses bisnis organisasi. Fokus utamanya adalah memastikan bahwa solusi yang dibangun atau diperoleh dapat memenuhi kebutuhan organisasi secara efektif.

d) DSS (*Deliver, Service and Support*)

Domain ini berhubungan dengan aktivitas operasional yang meliputi penyampaian layanan TI (delivery), pengelolaan layanan (service management), serta dukungan teknis (support) bagi pengguna. DSS memastikan bahwa layanan TI dapat beroperasi secara andal dan berkelanjutan.

e) MEA (*Monitor, Evaluate and Assess*)

Domain ini berfokus pada kegiatan pemantauan, evaluasi, dan penilaian kinerja TI, termasuk kepatuhan terhadap sasaran kinerja internal, tujuan pengendalian internal, dan persyaratan eksternal. Proses dalam domain ini membantu memastikan bahwa tata kelola TI selalu berada pada jalur yang benar serta sesuai regulasi yang berlaku.

Domain-domain yang telah dijelaskan sebelumnya merupakan faktor penting yang memberikan kontribusi signifikan terhadap efektivitas sistem tata kelola teknologi informasi di suatu perusahaan atau instansi. Selain domain, COBIT 2019 juga memuat komponen-komponen lain yang berperan dalam memperkuat dan mendukung penerapan tata kelola TI. Komponen tersebut mencakup berbagai

aspek yang saling melengkapi, mulai dari prinsip tata kelola, tujuan kinerja, proses inti, hingga panduan implementasi yang dirancang untuk memastikan keselarasan antara strategi TI dan tujuan organisasi. Komponen-komponen tersebut meliputi:

a) *Processes*

Proses merupakan serangkaian praktik dan aktivitas yang terorganisir untuk mencapai tujuan tertentu, menghasilkan keluaran (output) yang mendukung pencapaian sasaran terkait TI secara menyeluruh.

b) *Organizational Structure*

Struktur organisasi berfungsi sebagai entitas pengambil keputusan utama dalam perusahaan, memastikan peran dan tanggung jawab dalam tata kelola TI terdistribusi dengan jelas.

c) *Principles, Policies, and Procedures*

Prinsip, kebijakan, dan prosedur berperan dalam menerjemahkan perilaku yang diharapkan menjadi panduan praktis yang dapat diterapkan dalam pengelolaan dan operasional sehari-hari.

d) *Information*

Informasi tersebar di seluruh bagian organisasi dan mencakup semua data yang dihasilkan maupun digunakan oleh perusahaan. COBIT 2019 menitikberatkan pada informasi yang relevan untuk memastikan berfungsinya sistem tata kelola secara efektif.

e) *Culture, Ethics, and Behavior*

Budaya organisasi, etika, dan perilaku individu maupun kolektif merupakan faktor yang sering diabaikan, padahal memiliki pengaruh

signifikan terhadap keberhasilan implementasi tata kelola dan manajemen TI.

f) *People, Skills, and Competencies*

Sumber daya manusia, keterampilan, dan kompetensi yang memadai diperlukan untuk mendukung pengambilan keputusan yang tepat, pelaksanaan tindakan korektif, dan keberhasilan penyelesaian seluruh aktivitas tata kelola.

g) *Services, Infrastructure, and Applications*

Layanan, infrastruktur, dan aplikasi mencakup teknologi serta sistem pendukung yang menyediakan kemampuan pemrosesan informasi dan teknologi (I&T) bagi perusahaan, sekaligus menjadi fondasi bagi keberlangsungan tata kelola TI.

2.3.12 RACI Chart

RACI (*Responsible, Accountable, Consulted, and Informed*) merupakan kerangka kerja yang digunakan untuk menentukan peran dan tanggung jawab setiap fungsi dalam suatu organisasi, dengan tujuan memastikan tercapainya target yang telah ditetapkan. Penerapan skema RACI memungkinkan seluruh anggota organisasi atau instansi melaksanakan peran masing-masing secara terstruktur dan sistematis.

Dalam konteks tata kelola teknologi informasi, setiap process goal menerapkan skema RACI pada aktivitasnya. Hal ini dilakukan untuk memperjelas pembagian peran dan tanggung jawab, sekaligus menjadi sarana penentuan keterlibatan 26 fungsi jabatan terhadap suatu aktivitas tertentu. Di lapangan, skema

RACI terbukti membantu auditor dalam menyusun serta menyebarkan kuesioner secara tepat sasaran sesuai target dan fokus masing-masing posisi di instansi yang bersangkutan.

Adapun kriteria peran dalam skema RACI adalah sebagai berikut:

a) R – *Responsible*

Pihak yang bertugas memastikan suatu aktivitas terlaksana dengan baik dan mencapai hasil yang telah ditentukan.

b) A – *Accountable*

Pihak yang memiliki kewenangan akhir untuk menyetujui atau menerima pelaksanaan suatu aktivitas, serta bertanggung jawab penuh terhadap keberhasilannya.

c) C – *Consulted*

Pihak yang pendapat, masukan, atau keahliannya dibutuhkan dalam pelaksanaan suatu aktivitas. Komunikasi pada peran ini bersifat dua arah.

d) I – *Informed*

Pihak yang perlu selalu mendapatkan informasi terkini terkait kemajuan atau perkembangan suatu aktivitas. Komunikasi pada peran ini bersifat satu arah.

BAB 3
METODE PENELITIAN

3.1 Kondisi Eksisting dan Prosedur Operasional Saat Ini

Sebelum melakukan evaluasi menggunakan kerangka kerja COBIT 2019, esensial untuk memetakan kondisi eksisting dan menganalisis *Standar Operasional Prosedur* (SOP) yang berlaku di Kantor Sekretariat DPRD Kota Sorong. Analisis awal ini memberikan konteks empiris yang mendasari urgensi penelitian dan membantu memetakan praktik-praktik yang ada terhadap domain APO12 (*Managed Risk*).

3.1.1 Kondisi Eksisting Sebelum Evaluasi

Berdasarkan observasi awal dan wawancara pendahuluan di Kantor DPRD Kota Sorong, ditemukan bahwa manajemen risiko teknologi informasi saat ini berjalan secara implisit, reaktif, dan belum terstruktur, di mana tindakan perbaikan lebih sering dipicu setelah sebuah insiden terjadi, bukan berdasarkan analisis proaktif terhadap potensi ancaman. Hingga saat penelitian ini dilakukan, belum ditemukan adanya artefak formal yang menjadi fondasi manajemen risiko yang matang, seperti daftar risiko (*risk register*) yang terpusat dan dipelihara secara berkala, kebijakan formal, maupun mekanisme pelaporan risiko yang rutin dan terstandarisasi kepada pimpinan; peninjauan pada *Standar Operasional Prosedur* (SOP) yang ada juga menunjukkan ketiadaan prosedur yang secara khusus mengatur manajemen risiko TI. Akibatnya, kekuatan yang ada saat ini lebih bertumpu pada kapabilitas teknis dan pengalaman individual tim dalam merespons

insiden, bukan terlembagakan dalam sebuah siklus manajemen risiko yang formal dan berkelanjutan. Kondisi ini menjadi dasar dan justifikasi kuat mengapa evaluasi pada domain APO12 (*Managed Risk*) perlu dilakukan untuk membangun fondasi yang lebih sistematis.

3.1.2 Analisis Standar Operasional Prosedur yang Berjalan

Peninjauan mendalam terhadap *Standar Operasional Prosedur* (SOP) Sekretariat DPRD Kota Sorong menunjukkan bahwa institusi telah memiliki kematangan dalam standardisasi proses kerja pada level administratif dan operasional umum. Terdapat serangkaian prosedur yang telah terdefinisi dengan baik untuk berbagai aktivitas, seperti "Administrasi Surat Keluar", "Pengelolaan Arsip", dan "Penanganan Pengaduan". Keberadaan SOP ini mengindikasikan bahwa organisasi telah memahami pentingnya standardisasi untuk menjamin konsistensi dan kualitas layanan.

Namun, setelah dilakukan analisis konten yang spesifik, tidak ditemukan satu pun SOP yang secara eksplisit membahas atau mengatur tentang manajemen risiko teknologi informasi. Sebagai contoh, dalam "SOP Penanganan Pengaduan", alur kerja difokuskan pada penerimaan, pencatatan, dan respons terhadap keluhan dari masyarakat atau pihak internal. Prosedur tersebut tidak mencakup langkah untuk mengidentifikasi, menganalisis, atau melaporkan risiko TI yang mungkin menjadi akar penyebab dari sebuah aduan (misalnya, aduan karena sistem layanan publik tidak dapat diakses).

Ketiadaan SOP khusus yang mengatur siklus identifikasi, analisis, evaluasi, dan mitigasi risiko TI ini mengonfirmasi temuan dari observasi awal. Hal ini

menunjukkan adanya kesenjangan (gap) yang signifikan antara kebutuhan untuk mengamankan aset informasi digital dengan kerangka kerja prosedural yang ada. Kondisi ini menjadi justifikasi ilmiah yang kuat mengenai relevansi dan urgensi dilakukannya evaluasi pada domain APO12 untuk membangun fondasi manajemen risiko TI yang lebih sistematis dan matang.

3.2 Jenis, Sifat, dan Pendekatan Penelitian

Penelitian ini menerapkan pendekatan audit teknologi informasi dengan menggunakan kerangka kerja COBIT 2019 sebagai standar evaluasi. Secara spesifik, penelitian ini berfokus pada domain APO12 (Managed Risk) untuk menilai tingkat kapabilitas pengelolaan risiko TI dan menyusun rekomendasi perbaikan bagi Kantor DPRD Kota Sorong.

3.3 Proses Bisnis dan Alur Informasi Objek Penelitian

Untuk memahami konteks penerapan dan risiko Teknologi Informasi (TI), penting untuk memetakan proses bisnis inti yang berjalan di Kantor DPRD Kota Sorong. Pemetaan ini bertujuan untuk mengidentifikasi alur informasi kritis, titik-titik ketergantungan pada sistem TI, dan area-area di mana risiko dapat muncul dan berdampak signifikan terhadap fungsi kelembagaan. Sesuai dengan mandatnya, proses bisnis utama DPRD terbagi menjadi tiga fungsi inti:

1. Fungsi Legislasi (Pembentukan Peraturan Daerah)

   Ini adalah fungsi paling fundamental di mana DPRD menghasilkan produk hukum daerah. Alur informasinya sangat sensitif dan memerlukan integritas data yang tinggi di setiap tahap.

Tahapan Proses:

1. Penerimaan Aspirasi: Usulan dari masyarakat atau Pemerintah Daerah diterima dalam bentuk dokumen digital (email, portal) maupun fisik.
2. Penyusunan Naskah & Draf Raperda: Tim di Sekretariat DPRD dan anggota dewan menyusun naskah akademik dan draf awal Peraturan Daerah (Raperda). Proses ini sangat bergantung pada perangkat TI (komputer, jaringan internal) untuk pembuatan, penyimpanan, dan kolaborasi dokumen.
3. Di sinilah risiko integritas dan kerahasiaan data pertama kali muncul. Kebocoran draf Raperda dapat berdampak pada stabilitas politik dan hukum di daerah.
4. Pembahasan Internal: Draf dibahas di tingkat komisi dan fraksi. Risalah rapat dan notulensi digital dihasilkan, berisi data diskusi yang sensitif dan strategis.
5. Sidang Paripurna: Pengambilan keputusan final dilakukan dalam sidang paripurna yang hasilnya menjadi dokumen hukum resmi.
6. Publikasi: Peraturan Daerah yang telah disahkan dipublikasikan melalui kanal resmi, termasuk website DPRD. Hal ini menuntut ketersediaan dan keamanan sistem dari ancaman eksternal.

2. Fungsi Penganggaran (Persetujuan APBD)

Fungsi ini berkaitan dengan kewenangan DPRD dalam membahas dan menyetujui Anggaran Pendapatan dan Belanja Daerah (APBD) bersama pemerintah daerah.

Tahapan Proses:

1. Penerimaan Rancangan Anggaran: DPRD menerima dokumen rancangan anggaran dari Pemerintah Daerah, umumnya dalam format digital.
2. Analisis & Evaluasi: Anggota dewan dan staf ahli menganalisis usulan anggaran menggunakan aplikasi pengolah data. Risiko terkait akurasi dan validitas data menjadi krusial di tahap ini.
3. Rapat Pembahasan: Pembahasan detail dilakukan dalam rapat-rapat komisi dan badan anggaran, yang menghasilkan notulensi digital.
4. Persetujuan: Hasil akhir berupa dokumen persetujuan APBD yang sah secara hukum.

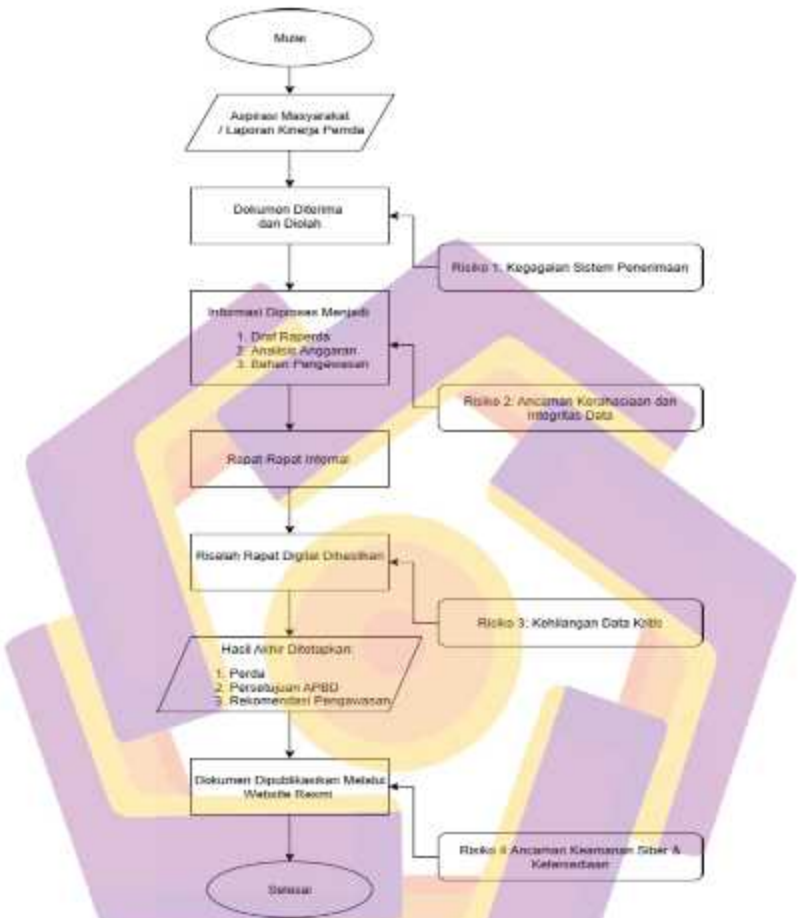
3. Fungsi Pengawasan (*Oversight*)

Fungsi ini bertujuan untuk mengawasi pelaksanaan kebijakan pemerintah daerah dan penggunaan APBD. Proses ini sangat bergantung pada analisis data yang akurat.

Tahapan Proses:

1. Penerimaan Laporan Kinerja: DPRD menerima laporan kinerja dan keuangan dari Pemerintah Daerah, seringkali dalam bentuk digital.
2. Analisis Laporan: Anggota dewan melakukan analisis terhadap laporan tersebut untuk menilai efektivitas kebijakan.
3. Rapat Dengar Pendapat (RDP): DPRD menyelenggarakan RDP dengan pihak eksekutif untuk meminta klarifikasi. Hasil rapat yang berupa risalah dan rekomendasi kembali menjadi aset informasi penting. Kegagalan sistem TI dapat menghambat fungsi pengawasan dan merusak citra serta kepercayaan publik.

Berdasarkan keterangan di atas, alur kerja dan informasi di Kantor DPRD Kota Sorong dapat divisualisasikan dalam flowchart berikut. Flowchart ini secara spesifik menyoroti titik-titik di mana manajemen risiko TI yang lemah dapat menyebabkan dampak negatif.



Gambar 3.1 Flowchart Proses Bisnis Kantor DPRD Kota Sorong

Pada gambar 3.1 di atas merupakan Flowchart proses bisnis pada Kantor DPRD Kota Sorong yang menunjukkan alur proses bisnis dan sirkulasi informasi kritis di lingkungan Kantor DPRD Kota Sorong. Tujuan utamanya adalah untuk memetakan secara sistematis tahapan-tahapan kerja dari penerimaan input eksternal hingga dihasilkannya output kebijakan, sekaligus mengidentifikasi titik-titik rentan

di mana risiko teknologi informasi (TI) dapat timbul dan berdampak signifikan terhadap fungsi kelembagaan. Berikut adalah penjelasan flowchart proses bisnis pada Kantor DPRD Kota Sorong :

1. Fase Input dan Pengolahan Awal

   Tahap ini dimulai dengan penerimaan data dari sumber eksternal yang menjadi pemicu proses legislatif.

   - Input Data: Proses diawali dengan adanya masukan data dari entitas eksternal, yaitu aspirasi dari masyarakat atau laporan kinerja dan rancangan anggaran dari Pemerintah Daerah. Input ini merupakan fondasi dari seluruh aktivitas DPRD.
   - Pengolahan Awal: Dokumen tersebut kemudian diterima dan diolah oleh Sekretariat DPRD. Pada titik ini, ketergantungan pada infrastruktur TI sangat tinggi.
   - Risiko 1: Kegagalan Sistem Penerimaan. Titik rentan pertama teridentifikasi di sini. Kegagalan pada sistem penerimaan digital (seperti server email atau portal aspirasi) dapat menyebabkan disrupsi total pada tahap awal, di mana informasi gagal masuk ke dalam alur kerja institusi.

2. Fase Proses Inti Internal

   Setelah data awal diterima, proses berlanjut ke tahap pengolahan internal di mana data mentah ditransformasikan menjadi produk legislatif yang strategis.

- Transformasi Informasi: Informasi yang masuk diproses menjadi dokumen kerja utama seperti Draf Rancangan Peraturan Daerah (Raperda), Analisis Anggaran, atau Bahan Pengawasan. Tahap ini merupakan proses intelektual inti lembaga.
- Risiko 2: Ancaman Kerahasiaan & Integritas Data. Ini merupakan titik risiko paling kritis. Draf Raperda dan analisis anggaran adalah aset informasi yang sangat sensitif. Tanpa manajemen risiko yang terstruktur, data ini rentan terhadap akses tidak sah, kebocoran, atau modifikasi ilegal, yang dapat berdampak pada stabilitas politik dan hukum. Kelemahan pada praktik APO12.03 (Memelihara Profil Risiko) secara langsung memperbesar ancaman ini.
- Deliberasi dan Dokumentasi: Dokumen-dokumen tersebut kemudian dibahas dalam rapat-rapat internal (komisi, fraksi, badan anggaran). Hasil dari deliberasi ini didokumentasikan dalam bentuk Risalah Rapat Digital.
- Risiko 3: Kehilangan Data Kritis. Risalah rapat adalah bukti otentik dari proses pengambilan keputusan. Ketiadaan prosedur pencadangan (*backup*) dan pemulihan bencana yang formal menempatkan dokumen krusial ini pada risiko kehilangan permanen akibat kegagalan teknis atau insiden lainnya.

3. Fase Finalisasi dan Publikasi

Tahap terakhir adalah formalisasi hasil kerja internal menjadi produk hukum atau kebijakan yang final dan mendiseminasikannya kepada publik.

- Penetapan Hasil Akhir: Hasil dari seluruh rangkaian proses internal ditetapkan menjadi output kebijakan final, seperti Peraturan Daerah (Perda), Persetujuan APBD, atau Rekomendasi Pengawasan.
- Diseminasi Publik: Dokumen final tersebut kemudian dipublikasikan melalui website resmi untuk memenuhi prinsip transparansi dan akuntabilitas publik.
- Risiko 4: Ancaman Keamanan Siber & Ketersediaan. Website sebagai kanal komunikasi utama dengan publik merupakan target serangan siber (misalnya, defacement, DDoS). Insiden keamanan atau ketidaktersediaan website pada saat publikasi dapat secara langsung mendelegitimasi institusi dan menunjukkan lemahnya mekanisme komunikasi risiko, yang terkait dengan praktik APO12.04 (Mengartikulasikan Risiko).

3.4 Metode Pengumpulan Data

Proses pengumpulan data dalam penelitian ini dilakukan dengan menggunakan beberapa metode yang dirancang secara sistematis untuk mendapatkan bukti-bukti yang relevan terkait evaluasi tata kelola risiko teknologi informasi di Kantor DPRD Kota Sorong, yaitu :

1. Wawancara: Wawancara semi-terstruktur dilakukan dengan para

pemangku kepentingan kunci di Kantor DPRD Kota Sorong yang memiliki peran dalam tata kelola dan operasional TI. Responden wawancara dipilih berdasarkan peran dan tanggung jawab Smereka, yang mencakup Pimpinan DPRD, Sekretaris Dewan (Sekwan), Kepala Bagian yang menangani TI, serta staf teknis terkait. Wawancara bertujuan untuk menggali pemahaman mendalam mengenai persepsi terhadap risiko, kebijakan yang ada, proses yang berjalan, dan tantangan yang dihadapi.

2. Kuesioner: Kuesioner terstruktur dikembangkan berdasarkan praktik-praktik manajemen yang terdapat dalam domain APO12 COBIT 2019. Kuesioner ini disebarkan kepada responden yang sama untuk mengukur tingkat implementasi dan kapabilitas dari setiap aktivitas pengelolaan risiko. Skala pengukuran yang digunakan mengacu pada model penilaian kapabilitas COBIT.
3. Studi Dokumentasi: Analisis dilakukan terhadap dokumen-dokumen internal organisasi yang relevan. Dokumen yang dikaji meliputi Rencana Strategis (Renstra) institusi, Standar Operasional Prosedur (SOP) terkait penggunaan dan keamanan TI, struktur organisasi, serta laporan atau catatan insiden. Tujuannya adalah untuk memverifikasi informasi yang diperoleh dari wawancara dan kuesioner, serta memahami kerangka kerja formal yang ada.
4. Observasi: Observasi langsung dilakukan untuk mengamati praktik pengelolaan risiko TI dalam kegiatan operasional sehari-hari. Metode

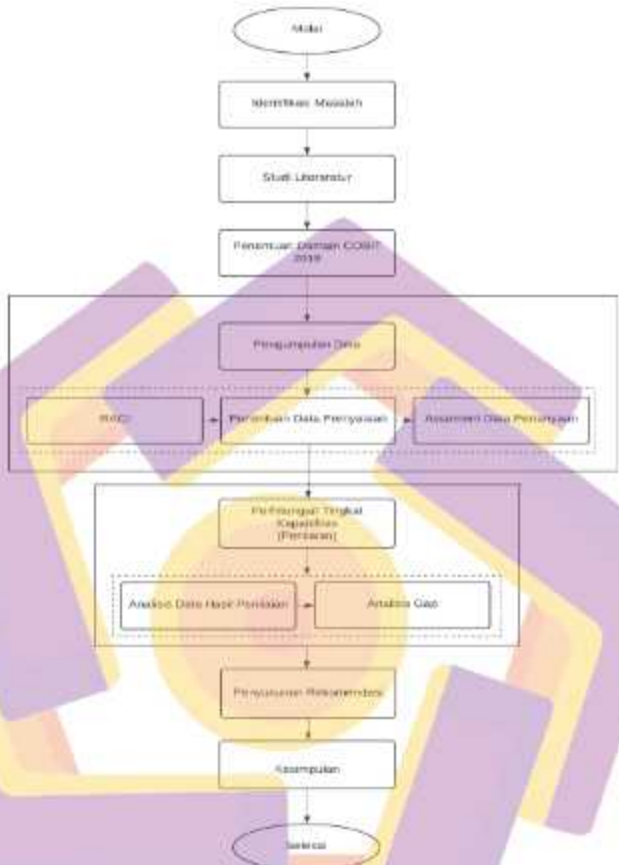
ini membantu memvalidasi apakah prosedur yang terdokumentasi benar-benar diimplementasikan di lapangan dan mengidentifikasi praktik-praktik informal yang mungkin belum tercatat.

3.5 Metode Analisis Data

Metode analisis data dalam penelitian ini mengadopsi pendekatan metode campuran (kuantitatif dan kualitatif) yang sistematis. Data kualitatif yang diperoleh dari wawancara dan studi dokumentasi akan dianalisis menggunakan teknik analisis konten untuk mengidentifikasi tema-tema kunci dan konteks penerapan manajemen risiko. Sementara itu, data kuantitatif dari kuesioner akan diolah untuk melakukan penilaian tingkat kapabilitas (*capability level assessment*) domain APO12. Hasil dari kedua analisis tersebut kemudian disintesiskan untuk melakukan analisis kesenjangan (*gap analysis*), yang pada akhirnya menjadi dasar untuk merumuskan rekomendasi perbaikan yang strategis dan aplikatif bagi Kantor DPRD Kota Sorong.

3.6 Alur Penelitian

Penelitian dilakukan dengan melalui beberapa tahapan proses yang sistematis. Alur dari penelitian dapat dilihat pada gambar 3.2 dimulai dari melakukan identifikasi masalah hingga mendapatkan rekomendasi dan kesimpulan.



Gambar 3.2 *Flowchart* Alur Penelitian

3.6.1 Identifikasi, Rumusan, Batasan dan Tujuan Penelitian

Metode analisis data dalam penelitian ini mengadopsi pendekatan metode campuran (kuantitatif dan kualitatif) yang sistematis. Data kualitatif yang diperoleh dari wawancara dan studi dokumentasi akan dianalisis menggunakan teknik analisis konten untuk mengidentifikasi tema-tema kunci dan konteks penerapan manajemen

risiko. Sementara itu, data kuantitatif dari kuesioner akan diolah untuk melakukan penilaian tingkat kapabilitas (*capability level assessment*) domain APO12. Hasil dari kedua analisis tersebut kemudian disintesiskan untuk melakukan analisis kesenjangan (*gap analysis*), yang pada akhirnya menjadi dasar untuk merumuskan rekomendasi perbaikan yang strategis dan aplikatif bagi Kantor DPRD Kota Sorong.

Tahap awal ini merupakan fondasi dari keseluruhan penelitian. Proses dimulai dengan observasi dan studi pendahuluan di Kantor DPRD Kota Sorong, yang mengidentifikasi peningkatan ketergantungan institusi pada teknologi informasi (TI) untuk mendukung fungsi legislasi, administratif, dan komunikasi. Ketergantungan ini secara simultan mengekspos organisasi terhadap berbagai risiko, seperti ancaman keamanan siber, kehilangan data, dan potensi ketidakpatuhan terhadap regulasi. Ditemukan bahwa evaluasi yang sistematis terhadap kerangka pengelolaan risiko TI di lingkungan institusi ini belum pernah dilakukan secara formal, sehingga menciptakan potensi kerentanan. Berdasarkan identifikasi tersebut, dirumuskan masalah-masalah penelitian utama:

a) Bagaimana tingkat kapabilitas pengelolaan risiko teknologi informasi di Kantor DPRD Kota Sorong berdasarkan framework COBIT 2019 domain APO12 (*Manage Risk*)?
b) Area proses manakah dalam domain APO12 yang menunjukkan kesenjangan (*gap*) kapabilitas paling besar antara kondisi aktual dengan kondisi target yang diharapkan?

c) Rekomendasi strategis apa yang dapat diberikan untuk meningkatkan pengelolaan risiko TI di Kantor DPRD Kota Sorong agar selaras dengan tujuan organisasi dan standar tata kelola TI?

Untuk memberikan kerangka metodologis yang presisi, penelitian ini diposisikan sebagai sebuah kegiatan evaluasi atau audit tata kelola TI dengan ruang lingkup dan batasan yang didefinisikan secara tegas: penelitian hanya dilakukan pada lingkup Kantor DPRD Kota Sorong dengan menggunakan framework COBIT 2019, dan secara spesifik berfokus pada domain APO12 (Managed Risk). Sesuai dengan posisinya sebagai kegiatan evaluasi, tujuan utama yang ingin dicapai adalah mengukur tingkat kapabilitas saat ini, mengidentifikasi kesenjangan terhadap tingkat target, dan menyusun rekomendasi perbaikan yang strategis dan aplikatif. Dengan demikian, fokus penelitian ini bukanlah pada implementasi teknis dari optimalisasi, melainkan pada perumusan sebuah panduan strategis yang berbasis bukti, terukur, dan dapat ditindaklanjuti oleh pihak manajemen di masa depan. Ruang lingkup dan batasan ini dapat dirinci sebagai berikut:

a) Apa yang Dioptimalkan? Target atau objek optimalisasi dalam penelitian ini adalah proses manajemen risiko TI di Kantor DPRD Kota Sorong, yang tercakup dalam domain COBIT 2019 APO12. Optimalisasi dalam konteks penelitian ini didefinisikan sebagai upaya terstruktur untuk meningkatkan tingkat kapabilitas (*capability level*) dari setiap proses yang dievaluasi. Peningkatan ini bertujuan untuk mentransformasikan proses dari kondisi saat ini (*as-is*) menuju kondisi target (*to-be*) yang lebih matang, terstruktur, proaktif, dan efektif, sesuai

dengan standar praktik terbaik yang diuraikan dalam kerangka kerja COBIT.

b) Bagaimana Optimalisasi Dirumuskan? Meskipun tidak melakukan implementasi, penelitian ini menghasilkan sebuah cetak biru (blueprint) untuk optimalisasi melalui serangkaian tahapan metodologis yang sistematis. Alur ini memastikan bahwa rekomendasi yang dihasilkan tidak bersifat umum, melainkan merupakan solusi yang dirancang khusus untuk menjawab kelemahan yang teridentifikasi. Tahapan tersebut adalah:

1. Evaluasi Kondisi Saat Ini: Tahap pertama adalah melakukan pengukuran tingkat kapabilitas aktual dari setiap proses dalam domain APO12. Kegiatan ini berfungsi sebagai baseline assessment untuk mengidentifikasi kekuatan dan, yang lebih penting, kelemahan fundamental dalam praktik manajemen risiko TI yang berjalan secara objektif.
2. Analisis Kesenjangan (*Gap Analysis*): Setelah kondisi saat ini dipetakan, dilakukan analisis kesenjangan dengan membandingkan hasil evaluasi tersebut dengan tingkat kapabilitas target yang telah ditetapkan (misalnya, Level 3). Analisis ini bertujuan untuk mengidentifikasi area-area yang memiliki kesenjangan paling signifikan dan, oleh karena itu, memerlukan prioritas perbaikan tertinggi.

3. Perumusan Rekomendasi Spesifik: Berdasarkan temuan dari analisis kesenjangan, dirumuskan rekomendasi yang bersifat konkret dan terperinci. Rekomendasi seperti pembuatan Risk Register terpusat dan penyusunan SOP Komunikasi Risiko secara langsung dirancang untuk menutup celah kapabilitas pada proses APO12.03 dan APO12.04.
4. Penyusunan Roadmap Implementasi: Sebagai tahap akhir, penelitian ini menyajikan sebuah peta jalan (*roadmap*) implementasi yang membagi proses perbaikan ke dalam fase-fase yang logis dan dapat dikelola (jangka pendek, menengah, dan panjang). Roadmap ini memberikan panduan praktis bagi manajemen mengenai langkah-langkah yang harus diambil, prioritas, dan estimasi waktu.

Dengan demikian penelitian ini, sesuai dengan alur metodologisnya, merupakan sebuah kegiatan evaluasi atau audit tata kelola TI, bukan sebuah proyek implementasi optimalisasi. Target optimalisasi dalam penelitian ini adalah proses manajemen risiko TI itu sendiri. Namun, penelitian ini tidak melakukan optimalisasi, melainkan menghasilkan sebuah cetak biru (blueprint) untuk optimalisasi melalui tahapan evaluasi kondisi saat ini, analisis kesenjangan, dan perumusan rekomendasi. Dengan demikian, output akhirnya bukanlah sebuah sistem yang telah dioptimalkan, melainkan sebuah dokumen analisis dan rekomendasi strategis, yang dapat digunakan oleh Kantor DPRD Kota Sorong

sebagai dasar yang valid untuk memulai inisiatif perbaikan proses manajemen risiko TI mereka di masa mendatang.

3.6.2 Studi Literatur

Pada tahap ini, dilakukan eksplorasi mendalam terhadap berbagai sumber referensi untuk membangun landasan teoretis yang kuat. Kajian literatur mencakup teori-teori mengenai tata kelola TI, manajemen risiko, kerangka kerja COBIT 2019, serta pendalaman khusus terhadap tujuan dan praktik dalam domain APO12 (Managed Risk). Selain itu, dilakukan peninjauan terhadap penelitian-penelitian sejenis yang telah dilakukan sebelumnya untuk memposisikan keaslian penelitian ini dan membandingkan temuan.

3.6.3 Pemilihan dan Justifikasi Domain Penelitian

Dalam domain manajemen risiko TI, terdapat beberapa kerangka kerja yang diakui secara global, seperti ISO/IEC 31000 yang menyediakan prinsip dan panduan umum untuk manajemen risiko, serta NIST *Risk Management Framework* (RMF) yang lebih preskriptif dan banyak digunakan oleh lembaga pemerintah federal AS. Meskipun framework tersebut sangat komprehensif, pemilihan COBIT 2019, dan secara spesifik domain APO12 (*Managed Risk*), dalam penelitian ini didasarkan pada beberapa kelebihan yang selaras dengan tujuan penelitian:

1. Fokus pada Tata Kelola (*Governance*): Berbeda dengan framework lain yang lebih berfokus pada operasional manajemen risiko, COBIT 2019 secara eksplisit menghubungkan manajemen risiko TI dengan pencapaian tujuan strategis organisasi. Ini sangat relevan untuk DPRD yang tujuannya bersifat strategis-politis.

2. Model Pengukuran Kematangan yang Terstruktur: COBIT 2019 menyediakan *Process Assessment Model* (PAM) yang jelas untuk mengukur tingkat kapabilitas (*capability level*) dari Level 0 hingga 5. Ini memungkinkan peneliti untuk melakukan benchmarking dan identifikasi kesenjangan (*gap*) secara kuantitatif dan terukur.
3. Komprehensif dan Holistik: Domain APO12 tidak hanya mencakup identifikasi dan analisis risiko, tetapi juga mencakup proses-proses krusial seperti pengumpulan data risiko (APO12.01), pemeliharaan profil risiko (APO12.03), dan komunikasi risiko (APO12.04), yang memungkinkan analisis yang lebih mendalam terhadap seluruh siklus manajemen risiko.

Pemilihan domain penelitian dalam kerangka kerja COBIT 2019 tidak dilakukan secara acak, melainkan merupakan sebuah keputusan metodologis yang didasarkan pada proses justifikasi berlapis. Proses ini melibatkan analisis masalah kontekstual, penentuan skala prioritas strategis, dan penyelarasan dengan tujuan institusional Kantor DPRD Kota Sorong. Dari 40 domain tata kelola dan manajemen yang tersedia, domain APO12 (*Managed Risk*) dipilih sebagai fokus tunggal dan utama penelitian ini dengan pertimbangan sebagai berikut:

1. Identifikasi Masalah Fundamental Berdasarkan Kondisi Eksisting

   Berdasarkan observasi awal dan analisis kondisi faktual, ditemukan bahwa praktik manajemen risiko teknologi informasi (TI) yang berjalan di institusi cenderung bersifat reaktif dan belum terstruktur. Pola kerja reaktif, di mana tindakan hanya dipicu setelah terjadinya sebuah insiden,

merupakan sebuah masalah fundamental dalam paradigma tata kelola TI modern. Pendekatan ini tidak hanya meningkatkan potensi kerugian akibat gangguan yang dapat dicegah, tetapi juga menunjukkan ketiadaan mekanisme proaktif untuk melindungi aset informasi. Tanpa adanya fondasi manajemen risiko yang solid, seluruh proses dan layanan TI lainnya mulai dari keamanan data hingga ketersediaan sistem menjadi rentan terhadap ancaman dan gangguan yang tidak terduga. Oleh karena itu, mengatasi kelemahan pada manajemen risiko menjadi prasyarat esensial sebelum melakukan evaluasi pada domain-domain lainnya.

2. Tingkat Urgensi Tertinggi Berdasarkan Konteks Institusional

   Dalam konteks lembaga publik seperti Kantor DPRD Kota Sorong, yang mengelola data legislatif yang bersifat sensitif, krusial, dan seringkali rahasia, domain manajemen risiko (APO12) secara inheren memiliki tingkat urgensi tertinggi. Potensi kegagalan dalam mengelola risiko TI dapat menimbulkan dampak yang jauh lebih besar daripada sekadar kerugian finansial; hal ini dapat mencakup dampak operasional (misalnya, kegagalan sistem saat sidang paripurna), dampak hukum (misalnya, kebocoran data rahasia negara), dan dampak reputasi (misalnya, menurunnya kepercayaan publik terhadap institusi). Jika dibandingkan dengan domain lain seperti APO04 (*Managed Innovation*) atau APO07 (*Managed Human Resources*), yang lebih berfokus pada optimalisasi dan pengembangan, domain APO12 berfokus pada perlindungan dan keberlangsungan (*preservation and*

continuity). Dengan demikian, membangun fondasi manajemen risiko yang kuat merupakan prioritas utama yang tidak dapat ditawar untuk menjamin stabilitas dan keamanan institusi.

3. Kesesuaian dengan Tujuan Strategis Institusi

   Tujuan strategis utama dari Kantor DPRD adalah menjamin kelancaran, keamanan, dan integritas dalam setiap proses legislatif. Domain APO12 secara langsung mendukung dan selaras dengan pencapaian tujuan strategis ini. Proses-proses di dalam APO12 mulai dari identifikasi dan pengumpulan data risiko (APO12.01), analisis risiko (APO12.02), hingga perencanaan dan implementasi respons risiko (APO12.05 & APO12.06) merupakan mekanisme instrumental untuk memastikan bahwa setiap potensi gangguan dari sisi teknologi dapat diidentifikasi, dinilai, dan ditangani secara proaktif sebelum sempat menimbulkan kerugian yang signifikan. Dengan kata lain, domain APO12 berfungsi sebagai garda terdepan dalam memastikan bahwa teknologi informasi benar-benar menjadi pendukung bagi tercapainya tujuan strategis institusi, bukan justru menjadi sumber masalah.

3.6.4 Pengumpulan Data

Pengumpulan data primer dilakukan dengan menggunakan pendekatan kuantitatif melalui teknik survei dengan penyebaran kuesioner. Kuesioner ini dirancang secara spesifik berdasarkan serangkaian aktivitas yang terdapat dalam enam subdomain APO12 (APO12.01 hingga APO12.06). Pengumpulan data bertujuan untuk mengukur secara faktual tingkat implementasi setiap praktik

manajemen risiko TI yang dijalankan oleh para pemangku kepentingan di Kantor DPRD Kota Sorong.

3.6.5 RACI Chart Kantor DPRD Kota Sorong

Pemetaan peran dan tanggung jawab yang terdefinisi dengan jelas merupakan salah satu faktor kunci dalam memastikan keberhasilan penerapan tata kelola teknologi informasi, khususnya pada proses manajemen risiko. Untuk menjamin bahwa setiap aktivitas dalam pengelolaan risiko TI pada domain APO12 (Managed Risk) terlaksana secara efektif, penelitian ini menerapkan pendekatan pemetaan peran melalui RACI Chart. RACI Chart digunakan untuk mengidentifikasi dan mendeskripsikan peran para pemangku kepentingan di Kantor DPRD Kota Sorong sesuai dengan fungsi dan tanggung jawab mereka dalam siklus manajemen risiko.

Berdasarkan hasil analisis struktur organisasi serta informasi yang diperoleh dari responden, disusunlah RACI Chart yang memetakan secara rinci pembagian peran dan tanggung jawab setiap pemangku kepentingan pada domain APO12 di Kantor DPRD Kota Sorong. Pemetaan ini tidak hanya bertujuan untuk memperjelas alur tanggung jawab, tetapi juga untuk meningkatkan koordinasi antarunit kerja dalam upaya meminimalkan risiko yang terkait dengan pengelolaan teknologi informasi. Melalui pemetaan ini, peran setiap pihak dikategorikan ke dalam empat tipe utama, yaitu:

1. R *(Responsible)* : Pihak yang secara langsung bertugas melaksanakan aktivitas atau proses yang berkaitan dengan manajemen risiko.

2. A *(Accountable)* : Pihak yang memiliki kewenangan akhir dan bertanggung jawab penuh atas keberhasilan pelaksanaan suatu proses atau aktivitas.
3. C *(Consulted)* : Pihak yang memberikan masukan, rekomendasi, atau pandangan melalui komunikasi dua arah untuk mendukung keberhasilan proses.
4. I *(Informed)* : Pihak yang menerima informasi secara berkala mengenai perkembangan atau hasil akhir suatu aktivitas melalui komunikasi satu arah.

Berikut adalah RACI Chart Kantor DPRD Kota Sorong yang terdapat pada Tabel 3.1 berikut ini.

Tabel 3.1 RACI Chart Kantor DPRD Kota Sorong

Peran COBIT 2019	Nama Responden	Jabatan	RACI
Legal Counsel	Regina AP, SH., MM	Kepala Bagian Hukum dan Persidangan	A
Program Manager	Gotlief Runpaisum, SE	Kasubag. Program dan Keuangan	R
Service Manager	Yanti Yumame, SH	Kasubag. Persidangan	R
Chief Financial Officer (CFO)	Fatmawati Djalali, S.IP., MM	Kabag. Keuangan	C
Business Process Owner	Ningsih Maryke Fonataba, SE	Kabag. Umum	I

3.6.6 Perhitungan Tingkat Kapabilitas

Tahap ini bertujuan untuk menjawab rumusan masalah pada poin C, yaitu mengonversi hasil evaluasi terhadap aktivitas dalam domain APO12 menjadi

rekomendasi yang dapat diimplementasikan secara praktis dan terukur. Proses pengolahan data dilakukan melalui pengklasifikasian status pelaksanaan setiap aktivitas berdasarkan enam subdomain APO12, yaitu sebagai berikut:

1. APO12.01 (*Collect and Maintain Risk Information*): Mengumpulkan data dan informasi risiko TI secara sistematis dan berkelanjutan untuk menjadi dasar analisis, pemantauan, dan strategi mitigasi.
2. APO12.02 (*Analyze Risk*): Mengevaluasi risiko yang teridentifikasi dengan mempertimbangkan kemungkinan, dampak, dan hubungan antar risiko untuk menetapkan prioritas penanganan.
3. APO12.03 (*Maintain Risk Profile*): Memperbarui dan memelihara profil risiko secara rutin agar selalu relevan dan akurat sesuai kondisi terkini organisasi.
4. APO12.04 (*Articulate Risk*): Menyampaikan informasi risiko secara jelas dan tepat waktu kepada pemangku kepentingan untuk memastikan pemahaman yang selaras.
5. APO12.05 (*Risk Response Planning*): Menyusun rencana penanganan risiko yang terukur, mempertimbangkan opsi mitigasi, biaya, sumber daya, dan tingkat urgensi.
6. APO12.06 (*Risk Response Implementation*): Melaksanakan rencana penanganan risiko secara terstruktur, memantau efektivitasnya, dan menyesuaikan strategi bila ada perubahan kondisi atau risiko baru.

3.6.7 Analisis Data Hasil Penilaian

Tahap ini merupakan fase krusial di mana data kuantitatif yang telah dikumpulkan melalui kuesioner diolah dan dianalisis secara sistematis untuk menentukan tingkat kapabilitas (*capability level*) aktual dari proses manajemen risiko TI di Kantor DPRD Kota Sorong. Penilaian ini mengacu secara ketat pada model kapabilitas proses dan skala penilaian yang didefinisikan dalam kerangka kerja COBIT 2019. Berdasarkan hasil perhitungan, tingkat kapabilitas domain APO12 (*Managed Risk*) secara keseluruhan teridentifikasi berada pada Level 2 (*Managed*).

Pencapaian pada Level 2 ini mengindikasikan bahwa proses-proses manajemen risiko TI telah diimplementasikan dan sebagian besar telah mencapai tujuannya. Namun, pelaksanaannya belum terkelola dengan baik secara menyeluruh. Terdapat fragmentasi kematangan proses, di mana beberapa aktivitas sudah berjalan efektif, sementara aktivitas krusial lainnya masih sangat lemah. Analisis lebih mendalam pada setiap praktik manajemen menunjukkan temuan yang bervariasi:

1. APO12.01: Proses pengumpulan informasi risiko TI telah dilakukan, namun belum mengikuti prosedur yang terdokumentasi dan terstandarisasi. Data risiko yang diperoleh cenderung bersifat parsial dan tidak terintegrasi secara sistematis, sehingga berpotensi mengurangi ketepatan analisis risiko di tahap berikutnya.
2. APO12.02: Kantor DPRD Kota Sorong telah memiliki kemampuan yang baik dalam menganalisis risiko yang telah teridentifikasi, dengan

mempertimbangkan aspek probabilitas, dampak, dan keterkaitan antar risiko. Proses analisis ini telah dilakukan secara menyeluruh dan mendalam sehingga dapat memberikan prioritas penanganan yang jelas.

3. APO12.03: Pemeliharaan profil risiko belum dilakukan secara berkala dan terstruktur. Tidak terdapat mekanisme resmi untuk memastikan pembaruan informasi risiko seiring dengan perubahan kondisi internal maupun eksternal organisasi, yang mengakibatkan potensi ketidaksesuaian antara profil risiko dengan situasi terkini.
4. APO12.04: Penyampaian informasi risiko kepada pemangku kepentingan masih bersifat terbatas dan belum terdokumentasi dengan baik. Mekanisme komunikasi yang ada belum mampu memastikan bahwa seluruh pihak yang relevan memahami secara menyeluruh karakteristik dan dampak risiko yang dihadapi.
5. APO12.05: Perencanaan penanganan risiko telah dilakukan dengan mempertimbangkan opsi mitigasi dan ketersediaan sumber daya. Namun, dokumen perencanaan ini belum sepenuhnya terintegrasi ke dalam kerangka kerja resmi, sehingga koordinasi lintas unit kerja dalam implementasinya masih perlu ditingkatkan.
6. APO12.06: Pelaksanaan rencana penanganan risiko telah berjalan, namun masih memerlukan penguatan dalam aspek pemantauan efektivitas tindakan dan penyesuaian strategi apabila terjadi perubahan situasi atau muncul risiko baru. Dokumentasi pelaksanaan juga perlu

ditingkatkan agar proses dapat dievaluasi secara komprehensif di masa mendatang.

3.6.8 Laporan Rekomendasi

Berdasarkan hasil analisis yang mengidentifikasi kesenjangan (*gap*) antara kondisi kapabilitas saat ini, yakni Level 2 (*Managed*), dengan tingkat kapabilitas yang diharapkan, yaitu Level 3 (*Established*), maka disusun serangkaian rekomendasi. Rekomendasi ini diprioritaskan untuk mengatasi kelemahan fundamental pada proses dokumentasi dan komunikasi, serta mengintegrasikannya dengan proses-proses yang sudah berjalan matang. Rekomendasi ini disusun secara spesifik untuk menjembatani kelemahan yang ditemukan pada praktik-praktik domain APO12 (*Managed Risk*) sebagai berikut:

1. Standardisasi Dokumentasi dan Penguatan Analisis Risiko : Direkomendasikan untuk melakukan formalisasi proses pengumpulan data dan dokumentasi risiko TI. Langkah ini diawali dengan mengembangkan sistem pencatatan data risiko yang terstruktur yang mencakup seluruh unit kerja serta membuat templat standar untuk identifikasi risiko dengan klasifikasi yang jelas. Selain itu, proses analisis risiko yang sudah matang (APO12.02) perlu diperkuat dengan mengembangkan model prediksi sederhana berbasis data historis insiden TI dan menyusun laporan analisis risiko berkala yang disertai rekomendasi mitigasi konkret.
2. Pemutakhiran Profil Risiko secara Berkala dan Terintegrasi : Untuk mengatasi kelemahan pada subdomain APO12.03, direkomendasikan

agar Kantor DPRD Kota Sorong menetapkan prosedur pemutakhiran profil risiko secara berkala, minimal setiap semester, untuk memastikan relevansinya dengan kondisi terkini. Idealnya, pemutakhiran ini didukung oleh pembangunan mekanisme otomatis untuk memantau perubahan profil risiko dan diintegrasikan dengan sistem informasi internal DPRD. Hal ini memastikan bahwa profil risiko menjadi dokumen hidup yang dinamis, bukan sekadar arsip statis.

3. Implementasi Komunikasi Risiko yang Proaktif dan Partisipatif : Kesenjangan signifikan pada subdomain APO12.04 menunjukkan perlunya transformasi komunikasi risiko dari yang bersifat reaktif menjadi proaktif. Direkomendasikan untuk mengembangkan dashboard informasi risiko yang dapat diakses oleh pemangku kepentingan terkait dan menyelenggarakan rapat koordinasi risiko bulanan. Selain itu, perlu dibentuk sistem notifikasi real-time untuk risiko-risiko kritis guna memastikan pengambilan keputusan yang cepat dan tepat. Pendekatan ini akan mengubah komunikasi menjadi lebih terbuka dan melibatkan semua pihak terkait dalam upaya mitigasi.
4. Optimalisasi Portofolio Tindakan Mitigasi dan Respons Risiko : Untuk meningkatkan efektivitas subdomain APO12.05 dan APO12.06, direkomendasikan penyusunan matriks prioritas tindakan mitigasi berbasis analisis dampak-biaya. Hal ini memastikan bahwa sumber daya yang terbatas dialokasikan pada risiko yang paling krusial. Selanjutnya, perlu dikembangkan skenario respons terstruktur untuk berbagai jenis

insiden risiko, yang dilengkapi dengan pelatihan dan simulasi berkala. Terakhir, perlu diciptakan sistem evaluasi untuk mengukur efektivitas tindakan mitigasi yang telah diimplementasikan, sehingga menjadi dasar bagi siklus perbaikan berkelanjutan.

3.6.9 Kesimpulan

Penelitian ini dilakukan untuk menjawab pertanyaan-pertanyaan yang telah dirumuskan sebelumnya, berdasarkan hasil evaluasi menyeluruh terhadap pengelolaan risiko TI pada domain APO12 (*Managed Risk*) di Kantor DPRD Kota Sorong dengan menggunakan kerangka kerja COBIT 2019. Hasil analisis menunjukkan bahwa tingkat kapabilitas (*capability level*) pengelolaan risiko TI pada domain APO12 saat ini berada pada Level 2 (*Managed*). Kondisi ini mengindikasikan bahwa proses manajemen risiko telah dikelola direncanakan dan dipantau namun pelaksanaannya belum merata dan belum terintegrasi menjadi sebuah siklus yang utuh. Kekuatan yang ada terletak pada kematangan proses analisis dan respons risiko, sedangkan kelemahan utama terlihat pada aspek fundamental pemeliharaan profil risiko dan komunikasi risiko yang masih belum terkelola dengan baik, sehingga memutus siklus manajemen risiko yang seharusnya berkelanjutan.

Berdasarkan temuan tersebut, disusun rekomendasi strategis yang berfokus pada tiga prioritas utama:

a) Formalisasi Proses dan Dokumentasi Risiko : Menetapkan dasar kebijakan dan prosedur formal untuk pengelolaan risiko TI, menyusun format standar pencatatan risiko, serta mulai melakukan pembaruan

profil risiko secara berkala untuk membangun fondasi pengelolaan risiko yang terdokumentasi.

b) Penguatan Mekanisme Komunikasi dan Kolaborasi Risiko : Membangun mekanisme komunikasi yang lebih terstruktur dan terdokumentasi antara unit kerja terkait, memastikan informasi risiko disampaikan secara tepat waktu dan dapat diakses oleh seluruh pemangku kepentingan, serta mulai mengintegrasikan saluran komunikasi internal.

c) Optimalisasi Portofolio Tindakan dan Respons Risiko : Menyusun daftar awal tindakan mitigasi untuk risiko yang telah diidentifikasi, merumuskan langkah respons sederhana yang dapat segera diimplementasikan pada insiden tertentu, dan mempersiapkan kerangka kerja pengembangan skenario mitigasi yang lebih komprehensif di tahap selanjutnya.

Implementasi rekomendasi ini diharapkan mampu mengubah pengelolaan risiko TI dari yang bersifat parsial dan reaktif menjadi lebih sistematis, proaktif, dan berbasis data. Penerapan strategi ini tidak hanya akan meningkatkan konsistensi dan efektivitas mitigasi risiko, tetapi juga memperkuat keselarasan antara pemanfaatan teknologi informasi dengan tujuan strategis Kantor DPRD Kota Sorong, sekaligus mendukung terwujudnya tata kelola yang transparan, akuntabel, dan dapat meningkatkan kepercayaan publik.

3.6.10 Selesai

Tahap ini menandai kulminasi dari seluruh rangkaian proses penelitian. Hasil akhir dari penelitian ini adalah sebuah laporan evaluasi yang sistematis dan

berbasis bukti, yang tidak hanya mengukur kondisi tata kelola risiko TI saat ini tetapi juga menyediakan panduan perbaikan yang terstruktur. Laporan ini diharapkan dapat memberikan kontribusi praktis yang signifikan bagi Kantor DPRD Kota Sorong sebagai dasar pengambilan keputusan dalam upaya mengoptimalkan manajemen risiko teknologi informasi.

BAB 4
HASIL PENELITIAN DAN PEMBAHASAN

Proses penelitian ini diawali dengan pemilihan domain COBIT 2019 yang dianggap paling relevan dengan konteks organisasi, dilanjutkan dengan tahap perencanaan asesmen yang memuat perumusan metodologi secara rinci. Selanjutnya, pengumpulan dan pengolahan data dilaksanakan secara sistematis untuk memastikan keakuratan serta kelengkapan informasi yang diperoleh. Data tersebut kemudian dianalisis secara mendalam guna mengidentifikasi kesenjangan dan peluang perbaikan, yang selanjutnya menjadi dasar dalam penyusunan rekomendasi strategis untuk mencapai kondisi tata kelola teknologi informasi yang optimal. Pada tahap akhir, disusun rekomendasi yang bersifat komprehensif, yang tidak hanya memberikan arah perbaikan namun juga berfungsi sebagai panduan praktis dalam penerapan tata kelola teknologi informasi di lingkungan organisasi.

4.1 Gambaran Umum Objek Penelitian

Objek yang menjadi studi kasus dalam penelitian ini adalah Kantor Dewan Perwakilan Rakyat Daerah (DPRD) Kota Sorong. Sebagai lembaga legislatif di tingkat daerah, institusi ini memegang peranan vital dalam fungsi pemerintahan, yang meliputi legislasi, penganggaran, dan pengawasan. Dalam menjalankan mandatnya, Kantor DPRD Kota Sorong sangat bergantung pada ketersediaan dan keandalan sistem Teknologi Informasi (TI) untuk mendukung berbagai kegiatan administratif, komunikasi internal dan eksternal, serta pengelolaan data yang krusial.

Konteks penelitian ini didasari oleh adanya peningkatan ketergantungan pada infrastruktur digital, yang secara simultan mengekspos institusi pada spektrum risiko yang luas, seperti ancaman keamanan siber, potensi kebocoran data, dan ketidakpatuhan terhadap regulasi. Meskipun TI telah menjadi komponen integral, evaluasi yang sistematis terhadap kerangka kerja pengelolaan risiko TI di lingkungan institusi ini belum pernah dilaksanakan secara formal. Oleh karena itu, penelitian ini diposisikan sebagai upaya untuk menyediakan pendekatan evaluasi yang terstruktur menggunakan kerangka kerja COBIT 2019, dengan tujuan akhir memastikan bahwa pengelolaan risiko TI dapat mendukung fungsi lembaga secara efektif, aman, transparan, dan akuntabel.

4.2 Hasil Pengumpulan Data

Tahap pengumpulan data merupakan fase krusial dalam penelitian ini, di mana data primer dihimpun secara langsung dari lapangan untuk memperoleh gambaran faktual mengenai kondisi manajemen risiko TI di Kantor DPRD Kota Sorong. Pelaksanaan tahap ini mengacu secara ketat pada metodologi yang telah dirancang pada Bab III, guna memastikan validitas dan reliabilitas data yang akan menjadi dasar bagi analisis tingkat kapabilitas. Alur untuk memperoleh temuan dan merumuskan rekomendasi dalam penelitian ini mengikuti tiga tahapan metodologis yang saling berkelanjutan:

1) Tahap Pertama adalah Pengumpulan Data Berbasis Bukti. Pada tahap ini, data dihimpun menggunakan pendekatan metode campuran, di mana data kuantitatif dari kuesioner diperkaya dan divalidasi dengan data

kualitatif dari wawancara serta studi dokumentasi . Validitas setiap temuan telah diperkuat melalui proses triangulasi sumber.

2) Tahap Kedua adalah Analisis Data dan Identifikasi Temuan. Data yang telah tervalidasi kemudian diolah untuk menghitung tingkat kapabilitas aktual dari setiap praktik manajemen. Hasil perhitungan inilah yang menjadi temuan kuantitatif utama penelitian, yang kemudian dianalisis secara kualitatif untuk mengidentifikasi pola dan mengerucut pada temuan fenomena 'paradoks kematangan'.
3) Tahap Ketiga adalah Analisis Kesenjangan dan Perumusan Rekomendasi. Temuan tingkat kapabilitas saat ini (*as-is*) dibandingkan dengan tingkat target (*to-be*) untuk melakukan analisis kesenjangan. Kesenjangan yang teridentifikasi, terutama yang terbesar dan paling fundamental, menjadi dasar langsung bagi perumusan rekomendasi strategis.

4.2.1 Metode dan Responden

Pengumpulan data primer dalam penelitian ini dilaksanakan dengan mengimplementasikan pendekatan metode campuran (*mixed methods*) yang menggabungkan wawancara, kuesioner, dan observasi. Tujuan dari pendekatan ini adalah untuk memperoleh data kualitatif yang mendalam guna memahami konteks, serta data kuantitatif yang terstruktur untuk melakukan pengukuran kapabilitas secara objektif.

1) Wawancara: Metode wawancara dilaksanakan dengan pendekatan semi-terstruktur. Tujuan utamanya adalah untuk menggali wawasan kualitatif, melakukan validasi silang terhadap jawaban kuesioner, dan memahami

konteks di balik praktik manajemen risiko yang berjalan. Wawancara difokuskan pada pemangku kepentingan dengan peran strategis dan operasional, khususnya pimpinan dan staf di lingkungan Sekretariat DPRD yang terlibat dalam pengelolaan dan operasional TI, untuk mendapatkan pemahaman yang mendalam mengenai tantangan, kebijakan, dan praktik yang ada.

2) Kuesioner: Instrumen utama untuk pengumpulan data kuantitatif adalah kuesioner terstruktur yang dirancang sesuai model kapabilitas COBIT 2019, spesifik untuk domain APO12 (*Managed Risk*). Kuesioner ini memiliki desain hierarkis yang menilai setiap praktik APO12 secara berjenjang dari Level 1 hingga Level 3, dan menggunakan skala peringkat standar (N, P, L, F) yang dilengkapi dengan kolom justifikasi bukti. Instrumen ini didistribusikan kepada responden kunci yang telah diidentifikasi memiliki keterlibatan atau pengetahuan relevan terhadap proses manajemen risiko TI di institusi.

4.3 Analisis Capabillity Level APO12

Dalam kerangka kerja COBIT 2019, evaluasi tingkat kapabilitas (capability level) pada proses tata kelola dan manajemen teknologi informasi, termasuk pada domain APO12 (Managed Risk), dilakukan dengan mengacu pada model Capability Maturity Model Integration (CMMI). Model ini berfungsi untuk mengukur sejauh mana suatu proses mampu memenuhi tujuan tata kelola dan manajemen yang telah ditetapkan, serta sejauh mana penerapannya telah terstandarisasi di lingkungan organisasi. Pada konteks penelitian ini, penilaian

diarahkan untuk mengidentifikasi tingkat kematangan penerapan manajemen risiko teknologi informasi di Kantor DPRD Kota Sorong, yang diklasifikasikan ke dalam enam tingkatan kapabilitas mulai dari Level 0 hingga Level 5, dengan deskripsi sebagai berikut:

1. Level 0 (*Incomplete Process)*

   Proses pengelolaan risiko belum memiliki kemampuan dasar yang memadai, pelaksanaannya tidak lengkap, serta belum terdokumentasi dengan baik sehingga tujuan manajemen risiko tidak dapat tercapai secara optimal.

2. Level 1 (*Performed Process)*

   Aktivitas pengelolaan risiko telah dilakukan namun bersifat tidak terstruktur, tidak konsisten, dan masih bergantung pada inisiatif individu. Dokumentasi maupun mekanisme kontrol belum berjalan secara formal.

3. Level 2 (*Managed Process)*

   Proses manajemen risiko telah dikelola secara terencana dan mencakup serangkaian aktivitas yang lengkap, meskipun pengendalian dan dokumentasi yang diterapkan masih pada tahap mendasar.

4. Level 3 (*Established Process)*

   Proses pengelolaan risiko telah terdefinisi secara formal dan dijalankan secara konsisten di seluruh bagian organisasi, dengan dukungan sumber daya yang memadai serta penerapan pendekatan yang proaktif dan terdokumentasi.

5. Level 4 (*Predictable Process)*

   Proses pengelolaan risiko tidak hanya terdokumentasi dengan baik, tetapi juga dipantau menggunakan indikator kinerja terukur. Pemantauan ini memungkinkan pengendalian terhadap variabilitas serta peningkatan efektivitas dan efisiensi proses.

6. Level 5 (*Optimizing Process)*

   Proses pengelolaan risiko telah mencapai tingkat kematangan tertinggi, di mana perbaikan berkelanjutan dan inovasi dilakukan secara sistematis berdasarkan evaluasi kinerja serta masukan dari berbagai pemangku kepentingan.

Dalam mengukur tingkat kapabilitas pada domain APO12 di Kantor DPRD Kota Sorong, digunakan pendekatan rating process activities yang menilai sejauh mana setiap aktivitas proses dilaksanakan sesuai standar. Kriteria penilaian tersebut dikategorikan menjadi empat tingkat, yaitu:

1. *Fully Achieved*: Pencapaian lebih dari 85%, menunjukkan proses telah matang dan siap ditingkatkan ke level berikutnya.
2. *Largely Achieved*: Pencapaian antara 50% hingga 85%, menunjukkan proses telah berjalan dengan baik namun masih memerlukan penyempurnaan.
3. *Partially Achieved*: Pencapaian antara 15% hingga 50%, menandakan adanya kekurangan signifikan yang perlu segera dibenahi.
4. *Not Achieved*: Pencapaian kurang dari 15%, menunjukkan bahwa proses belum berjalan sesuai harapan dan memerlukan perbaikan mendasar.

Pendekatan ini memastikan bahwa peningkatan tingkat kapabilitas pada APO12 dilakukan secara sistematis, terukur, dan berbasis bukti, sehingga dapat mendukung penguatan tata kelola risiko teknologi informasi di Kantor DPRD Kota Sorong secara berkelanjutan.

4.3.1 Proses Perhitungan Tingkat Kapabilitas

Proses perhitungan tingkat kapabilitas dalam penelitian ini mengadopsi model kapabilitas proses yang terdapat dalam kerangka kerja COBIT 2019, yang secara metodologis selaras dengan pendekatan CMMI. Model ini bersifat hierarkis, mengklasifikasikan kematangan proses ke dalam enam tingkatan (Level 0 hingga 5). Untuk memastikan objektivitas dan pertanggungjawaban ilmiah, penilaian dilakukan secara progresif. Progresi ini dapat dianalogikan seperti menaiki tangga, di mana suatu proses harus menunjukkan pencapaian yang mapan pada satu level sebelum dapat dinilai pada level berikutnya.

Data peringkat kuantitatif (N/P/L/F) yang dihimpun dari kuesioner menjadi dasar untuk melakukan evaluasi ini. Setiap level kapabilitas memiliki serangkaian atribut proses yang harus dipenuhi. Suatu proses dinyatakan telah mencapai level kapabilitas tertentu apabila seluruh atribut proses pada level tersebut setidaknya memperoleh peringkat *Largely* (L), dengan syarat bahwa level di bawahnya telah tercapai secara *Fully* (F). Penerapan metodologi yang ketat ini sangat esensial untuk menjamin bahwa hasil penilaian yang diperoleh bersifat valid dan dapat dipertanggungjawabkan. Penentuan tingkat kapabilitas (*capability level*) untuk setiap proses dalam domain APO12 dilakukan secara sistematis dan hierarkis sesuai dengan panduan COBIT 2019 Process Assessment Model (PAM). Proses ini tidak

hanya berdasarkan rata-rata, tetapi juga pada pemenuhan syarat di setiap level secara berurutan. Berikut adalah contoh perhitungan detail untuk salah satu proses, APO12.01 (Mengumpulkan Data Risiko) :

1. Tahap 1: Perhitungan Kapabilitas per Praktik Manajemen.

   Penilaian dilakukan secara berjenjang. Sebuah praktik harus terbukti memenuhi kriteria pada satu level sebelum dapat dinilai pada level berikutnya.

   a. Evaluasi Level 1 (*Performed*):

      - Atribut proses pada Level 1 (PA 1.1) dievaluasi berdasarkan pertanyaan kuesioner mengenai apakah institusi telah melaksanakan aktivitas pengumpulan data risiko.
      - Hasil: Berdasarkan bukti dari kuesioner dan wawancara, mayoritas responden memberikan peringkat 'F' (*Fully Achieved*), yang mengindikasikan bahwa aktivitas dasar ini telah dilaksanakan secara konsisten.
      - Kesimpulan: Dengan tercapainya peringkat minimal 'L' (*Largely Achieved*), maka Level 1 dinyatakan terpenuhi.

   b. Evaluasi Level 2 (*Managed*):

      - Level ini memiliki dua atribut: PA 2.1 (Manajemen Kinerja) dan PA 2.2 (Manajemen Hasil Kerja). Keduanya harus terpenuhi.

- Hasil PA 2.1: Berdasarkan bukti adanya notulensi rapat yang menunjukkan adanya perencanaan dan pemantauan, atribut ini dinilai 'L' (*Largely Achieved*).
- Hasil PA 2.2: Output dari proses, seperti daftar sumber risiko, juga dinilai telah dikelola dengan baik, sehingga atribut ini dinilai 'L' (*Largely Achieved*).
- Kesimpulan: Karena kedua atribut pada Level 2 telah mencapai peringkat minimal 'L', maka Level 2 dinyatakan terpenuhi.

c. Evaluasi Level 3 (*Established*):

- Atribut proses pada Level 3 (PA 3.1 dan PA 3.2) mengevaluasi apakah proses telah terdefinisi dengan baik dan terstandarisasi (misalnya melalui SOP).
- Hasil: Berdasarkan wawancara dan studi dokumen, ditemukan bahwa belum ada SOP yang disahkan secara formal untuk proses pengumpulan data risiko. Oleh karena itu, atribut ini dinilai 'P' (*Partially Achieved*).
- Kesimpulan: Karena tidak mencapai peringkat minimal 'L', maka Level 3 dinyatakan tidak terpenuhi.

2. Tahap 2: Perhitungan Kapabilitas Domain Secara Keseluruhan.

Setelah tingkat kapabilitas keenam praktik ditetapkan, level domain secara keseluruhan dihitung melalui agregasi kuantitatif. Level dari setiap praktik dikonversi ke nilai numerik (Level 1=1, Level 2=2, Level 3=3), kemudian dihitung rata-ratanya.

Perhitungan Rata-rata: Total nilai (2+3+1+1+3+3) = 13. Nilai Rata-rata: 13 / 6 = 2.17.

Penetapan Level Akhir: Nilai rata-rata 2.17 dibulatkan ke bilangan bulat terdekat, yaitu 2.

Dengan demikian, tingkat kapabilitas domain APO12 (*Managed Risk*) secara keseluruhan ditetapkan pada Level 2 (*Managed*). Metodologi terstruktur ini memastikan hasil akhir didasarkan pada penilaian hierarkis yang ketat untuk setiap komponennya.

4.3.2 Proses Perhitungan Tingkat Kapabilitas

Kredibilitas dan keabsahan hasil perhitungan tingkat kapabilitas di atas sangat bergantung pada validitas data yang dikumpulkan. Untuk memastikan bahwa data yang menjadi dasar analisis adalah valid dan dapat dipertanggungjawabkan, diterapkan teknik triangulasi sumber. Triangulasi sumber merupakan metode pengujian validitas yang dilakukan dengan cara membandingkan dan mengecek ulang derajat kepercayaan suatu informasi yang diperoleh melalui sumber yang berbeda (Sugiyono, 2018).

Dalam konteks penelitian ini, proses triangulasi sumber dilaksanakan secara sistematis melalui tiga langkah verifikasi silang (*cross-verification*) untuk setiap temuan kunci:

1) Validasi Antar-Responden: Data yang diperoleh dari kuesioner satu responden (misalnya, yang memiliki peran *Accountable*) dibandingkan dengan data dari responden lain (misalnya, yang memiliki peran Responsible atau Informed). Langkah ini bertujuan untuk menguji

konsistensi pemahaman dan persepsi terhadap proses yang sama dari sudut pandang yang berbeda. Adanya kesamaan jawaban atau bukti yang saling mendukung antar responden memperkuat validitas temuan.

2) Validasi Kuesioner dengan Wawancara Mendalam: Temuan dari hasil kuesioner tidak diterima begitu saja. Setiap temuan kunci, terutama pada area dengan penilaian yang sangat tinggi atau sangat rendah, dikonfirmasi dan diperdalam melalui sesi wawancara semi-terstruktur. Sebagai contoh, ketika kuesioner menunjukkan kelemahan pada proses APO12.03 (Memelihara Profil Risiko), pertanyaan lanjutan diajukan saat wawancara untuk menggali penyebabnya, seperti "Apakah saat ini institusi telah memiliki dokumen risk register yang formal?". Jawaban dari wawancara ini digunakan untuk memvalidasi dan memberikan konteks pada data kuesioner.
3) Validasi Wawancara dengan Bukti Dokumenter: Pernyataan atau klaim yang muncul selama sesi wawancara kemudian diverifikasi dengan bukti fisik yang ada. Misalnya, jika seorang responden menyatakan bahwa "proses analisis risiko sudah terkelola dengan baik dan dibuktikan dengan adanya notulensi rapat", maka peneliti akan meminta untuk meninjau dokumen notulensi tersebut. Kesesuaian antara pernyataan verbal dengan bukti dokumenter menjadi lapisan validasi terakhir yang paling kuat.

Dengan menerapkan ketiga langkah triangulasi sumber ini, data yang digunakan dalam penelitian ini telah melalui proses verifikasi berlapis. Hal ini memastikan bahwa hasil perhitungan tingkat kapabilitas dan kesimpulan yang

ditarik tidak hanya berdasarkan persepsi subjektif, melainkan didasarkan pada data yang kredibel, konsisten, dan dapat dibuktikan kebenarannya.

4.3.3 Proses Perhitungan Tingkat Kapabilitas

Berdasarkan analisis data yang terkompilasi, tingkat kapabilitas domain APO12 (*Managed Risk*) di Kantor DPRD Kota Sorong secara keseluruhan teridentifikasi berada pada tingkatan Level 2 (*Managed*). Klasifikasi pada Level 2 ini merefleksikan bahwa proses manajemen risiko telah diimplementasikan secara terkelola artinya proses telah direncanakan, dipantau, dan disesuaikan. Namun, pelaksanaannya belum menjadi sebuah standar yang mapan dan terintegrasi di seluruh organisasi. Terdapat fragmentasi kematangan, di mana institusi menunjukkan kekuatan pada aspek teknis analisis dan respons, namun sangat lemah pada aspek fundamental dokumentasi dan komunikasi. Berikut adalah tabel 4.1 yang menyajikan ringkasan hasil penilaian tingkat kapabilitas untuk setiap praktik dalam domain APO12.

Tabel 4.1 Ringkasan Hasil Penilaian Tingkat Kapabilitas APO12

ID Praktik	Nama Praktik Manajemen	Tingkat Kapabilitas Akhir
APO12.01	Mengumpulkan Data Risiko	Level 2
APO12.02	Menganalisis Risiko	Level 3
APO12.03	Memelihara Profil Risiko	Level 1
APO12.04	Mengartikulasikan Risiko	Level 1
APO12.05	Merencanakan Tanggapan Risiko	Level 3
APO12.06	Mengimplementasikan Tanggapan Risiko	Level 3

4.3.4 Pembahasan Temuan Per-praktik APO12

1. APO12.01 (Mengumpulkan Data Risiko) - Level 2: Proses ini telah mencapai Level 2. Evidensi menunjukkan bahwa aktivitas pengumpulan data risiko telah direncanakan dan dijalankan. Namun, proses ini belum dapat mencapai Level 3 karena belum sepenuhnya terstandardisasi. Bukti seperti "prosedur formal belum disosialisasikan sepenuhnya" dan "data risiko belum tersimpan dalam repositori terpusat yang konsisten" menunjukkan bahwa proses ini sudah dikelola namun belum menjadi standar yang mapan.
2. APO12.02 (Menganalisis Risiko) Level 3: Praktik ini merupakan salah satu kekuatan utama dan berhasil mencapai Level 3. Terdapat bukti kuat adanya metode analisis risiko yang terdefinisi dengan baik dan diterapkan secara konsisten. Evidensi seperti "dokumen metodologi analisis risiko formal" dan "laporan prioritas mitigasi risiko" mengonfirmasi bahwa proses ini telah mapan (established) dan menjadi bagian dari praktik standar.
3. APO12.03 (Memelihara Profil Risiko) Level 1: Praktik ini teridentifikasi sebagai kelemahan kritis dan hanya berada di Level 1. Defisiensi utama yang menghambat progresi ke Level 2 adalah ketiadaan risk register atau profil risiko yang dipelihara secara formal dan berkala. Bukti dari responden secara konsisten menyatakan "tidak ada dokumen profil risiko yang diperbarui secara rutin," yang

mengindikasikan bahwa proses ini hanya dilakukan secara dasar (performed) dan belum dikelola.

4. APO12.04 (Mengartikulasikan Risiko) Level 1: Sama seperti sebelumnya, praktik ini terkualifikasi pada Level 1. Kelemahan fundamental terletak pada tidak adanya mekanisme komunikasi risiko yang terstruktur. Bukti seperti "pelaporan risiko hanya jika ada insiden" dan "tidak ada format laporan yang seragam" menunjukkan bahwa komunikasi risiko masih bersifat ad-hoc dan reaktif, belum dikelola secara proaktif.
5. APO12.05 (Merencanakan Tanggapan Risiko) Level 3: Praktik ini juga menunjukkan tingkat kematangan yang tinggi dan mencapai Level 3. Institusi memiliki proses yang terdefinisi dengan baik untuk merencanakan tindakan mitigasi. Bukti adanya "dokumen rencana mitigasi risiko" dan "laporan analisis biaya-manfaat" mengonfirmasi bahwa proses perencanaan respons risiko telah mapan dan terstandardisasi.
6. APO12.06 (Mengimplementasikan Tanggapan Risiko) Level 3: Proses ini juga teridentifikasi sebagai kekuatan pada Level 3. Institusi menunjukkan kemampuan untuk menjalankan rencana mitigasi risiko secara efektif dan konsisten. Evidensi berupa "laporan implementasi mitigasi risiko" yang terdokumentasi dengan baik menunjukkan bahwa proses ini telah mapan dan output-nya dapat diprediksi.

4.3.5 Analisis Tingkat Kematangan di Kantor DPRD Kota Sorong

Berdasarkan hasil penelitian yang menunjukkan tingkat kapabilitas domain APO12 secara keseluruhan berada pada Level 2 (*Managed*), maka tingkat kematangan (*maturity level*) manajemen risiko TI di Kantor DPRD Kota Sorong dapat ditetapkan pada Level 2 (Managed). Penetapan ini didasarkan pada justifikasi berikut:

1. Proses Sudah Terkelola: Sebagian besar proses telah diimplementasikan dan dikelola untuk mencapai tujuannya, seperti yang ditunjukkan oleh pencapaian Level 2 atau lebih tinggi pada lima dari enam praktik yang ada. Hal ini sesuai dengan karakteristik utama dari Maturity Level 2.
2. Belum Menjadi Standar Organisasi: Adanya dua praktik fundamental (APO12.03 dan APO12.04) yang masih berada di Level 1 menunjukkan bahwa proses manajemen risiko belum terstandardisasi dan terdefinisi dengan baik di seluruh organisasi. Kelemahan ini menghalangi institusi untuk mencapai
3. Maturity Level 3 (*Defined*), yang mensyaratkan adanya proses yang mapan dan terstandardisasi. Ketergantungan pada Proses Tertentu: Keberhasilan manajemen risiko saat ini lebih banyak ditopang oleh kekuatan pada proses analisis dan respons, bukan oleh sebuah siklus terintegrasi yang terdokumentasi dengan baik.

Dengan demikian, dapat disimpulkan bahwa Kantor DPRD Kota Sorong telah melewati tahap awal dan berada pada tahap di mana prosesnya telah dikelola

(*Managed*), namun masih memerlukan upaya standardisasi dan integrasi yang signifikan untuk mencapai tingkat kematangan yang lebih tinggi.

4.4 Analisis Kesenjangan (*Gap Analysis*)

Setelah tingkat kapabilitas saat ini berhasil ditetapkan, langkah selanjutnya dalam analisis adalah melakukan analisis kesenjangan (*gap analysis*). Tahap ini bertujuan untuk mengukur secara kuantitatif dan kualitatif selisih antara kondisi aktual (*as-is*) dari manajemen risiko TI di Kantor DPRD Kota Sorong dengan kondisi ideal atau target yang diharapkan (*to-be*). Analisis kesenjangan ini merupakan jembatan krusial yang menghubungkan antara temuan penelitian dengan perumusan rekomendasi yang strategis dan tepat sasaran.

4.4.1 Perbandingan Tingkat Kapabilitas

Perbandingan ini dilakukan untuk memetakan posisi Kantor DPRD Kota Sorong saat ini terhadap standar kematangan proses yang lebih ideal dalam mengelola risiko TI, yaitu :

a) Tingkat Kapabilitas Saat Ini (*As-Is*)

Seperti yang telah diuraikan pada sub-bab 4.3, hasil analisis data menunjukkan bahwa tingkat kapabilitas domain APO12 secara keseluruhan berada pada Level 2 (*Managed*). Hasil ini merefleksikan bahwa institusi telah mengelola proses manajemen risiko artinya proses telah direncanakan, dipantau, dan disesuaikan. Namun, terdapat paradoks kematangan yang signifikan: institusi menunjukkan kekuatan dan kapabilitas matang (Level 3) pada aspek teknis seperti analisis dan respons risiko, namun pada saat yang sama sangat lemah (Level 1) pada

aspek fundamental yaitu pemeliharaan profil risiko dan komunikasi risiko.

b) Tingkat Kapabilitas Target (*To-Be*)

Target tingkat kapabilitas yang realistis dan strategis untuk Kantor DPRD Kota Sorong dalam jangka menengah adalah Level 3 (*Established*). Penetapan target ini didasarkan pada justifikasi bahwa Level 3 merepresentasikan suatu kondisi di mana proses manajemen risiko tidak hanya dikelola, tetapi telah terstandardisasi, proaktif, dan terlembagakan di seluruh unit organisasi. Mencapai Level 3 akan secara langsung mengatasi kelemahan fundamental yang teridentifikasi, seperti ketiadaan profil risiko yang terstruktur dan mekanisme komunikasi risiko yang formal.

Berikut adalah tabel 4.2 yang menyajikan perbandingan dan kesenjangan tingkat kapabilitas APO12 sebagai berikut :

Tabel 4.2 Perbandingan dan Kesenjangan Tingkat Kapabilitas APO12

ID Praktik	Nama Praktik Manajemen	Kapabilitas Saat Ini *(As-Is)*	Kapabilitas Target *(To-Be)*	Kesenjangan *(Gap)*
APO12.01	Mengumpulkan Data Risiko	Level 2	Level 3	Level 1
APO12.02	Menganalisis Risiko	Level 3	Level 3	Level 0
APO12.03	Memelihara Profil Risiko	Level 1	Level 3	Level 2
APO12.04	Mengartikulasikan Risiko	Level 1	Level 3	Level 2
APO12.05	Merencanakan Tanggapan Risiko	Level 3	Level 3	Level 0
APO12.06	Mengimplementasikan Tanggapan Risiko	Level 3	Level 3	Level 0

4.4.2 Implikasi Kesenjangan

Kesenjangan kapabilitas yang teridentifikasi pada domain APO12 (*Managed Risk*) tidak hanya merepresentasikan perbedaan numerik antara kondisi saat ini (*as-is*) dan kondisi yang ditargetkan (*to-be*), tetapi juga mengandung implikasi strategis dan operasional yang signifikan terhadap efektivitas pengelolaan risiko teknologi informasi. Apabila kesenjangan ini tidak segera diatasi, maka akan timbul risiko keberlanjutan operasional, kelemahan dalam pengendalian internal, serta penurunan kemampuan organisasi untuk merespons ancaman secara tepat waktu dan terukur. Berikut adalah tabel 4.3 yang menyajikan ringkasan implikasi kesenjangan untuk setiap area praktik manajemen yang dianalisis.

Tabel 4.3 Implikasi Kesenjangan Tingkat Kapabilitas APO12

Praktik	Deskripsi Kesenjangan	Implikasi bagi Institusi
APO12.01 Mengumpulkan Data Risiko	Proses pengumpulan dan pemeliharaan informasi risiko berada pada Level 1 (reaktif dan belum terdokumentasi formal), sedangkan targetnya Level 3 (terstandardisasi dan terdokumentasi penuh).	1. Inkonsistensi Data Risiko: Data risiko tidak konsisten dan sulit diverifikasi, sehingga menghambat proses analisis risiko yang akurat. 2. Kelemahan Dasar Manajemen Risiko: Tanpa format dan mekanisme pencatatan baku, potensi risiko baru sulit diidentifikasi secara proaktif.
APO12.02 Menganalisis Risiko	Proses analisis risiko telah berada di Level 2 (terkelola secara operasional), namun belum mencapai Level 3 karena belum ada metodologi formal yang terdokumentasi.	1. Kurangnya Standarisasi Analisis: Perbedaan metode antar unit menyebabkan hasil

		analisis yang bervariasi. 2. Kesulitan Integrasi Data Risiko: Hasil analisis sulit diakumulasikan menjadi gambaran risiko organisasi secara menyeluruh.
APO12.03 Memelihara Profil Risiko	Profil risiko berada pada Level 1 dengan pembaruan yang tidak terjadwal dan tanpa format baku. Target adalah Level 3 yang mencakup pembaruan berkala dan penyimpanan terpusat.	1. Profil Risiko Tidak Mutakhir: Informasi risiko menjadi usang dan tidak relevan. 2. Keterbatasan Referensi untuk Pengambilan Keputusan: Manajemen tidak memiliki gambaran terkini mengenai risiko prioritas.
APO12.04 Mengartikulasikan Risiko	Proses penyampaian informasi risiko masih pada Level 1, dilakukan secara informal dan bergantung pada inisiatif individu.	1. Risiko Salah Persepsi: Pemangku kepentingan tidak menerima informasi risiko yang lengkap dan akurat. 2. Koordinasi Lemah: Keterlambatan dalam komunikasi berpotensi memperlambat respons terhadap insiden.
APO12.05 Menentukan Respons Risiko	Proses perencanaan mitigasi berada di Level 2, namun belum ada kerangka kerja resmi untuk menyusun portofolio tindakan mitigasi yang komprehensif.	1. Tindakan Mitigasi Tidak Konsisten: Implementasi mitigasi bergantung pada pengalaman individu. 2. Kesulitan Evaluasi Efektivitas: Tidak ada tolok ukur baku untuk mengukur keberhasilan mitigasi.
APO12.06	Proses respons risiko masih di Level 1, dilakukan tanpa prosedur	1. Respons Tidak Terkoordinasi: Tindakan yang

Menangani Risiko	standar dan tidak terdokumentasi dengan baik.	diambil dapat tumpang tindih atau saling bertentangan. 2. Potensi Kerugian Lebih Besar: Penanganan yang terlambat atau tidak tepat dapat memperburuk dampak risiko.

4.4.3 Justifikasi Prioritas Analisis dan Rekomendasi pada Praktik Fundamental

Hasil analisis kesenjangan pada Tabel 4.2 diatas secara kuantitatif menunjukkan bahwa kesenjangan terbesar memang terdapat pada praktik APO12.03 (Memelihara Profil Risiko) dan APO12.04 (Mengartikulasikan Risiko). Namun, penetapan kedua praktik ini sebagai fokus utama temuan dan prioritas rekomendasi tidak hanya didasarkan pada besaran gap atau rendahnya tingkat kapabilitas (Level 1) semata. Alasan yang lebih fundamental terletak pada peran strategis kedua praktik tersebut sebagai fondasi dan penghubung dalam siklus manajemen risiko. Berdasarkan analisis, ditemukan bahwa kegagalan pada kedua praktik ini menjadi akar masalah yang menyebabkan "siklus manajemen risiko terputus". Justifikasinya adalah sebagai berikut:

1) Peran APO12.03 sebagai Pusat Memori Organisasional: Praktik APO12.03 berfungsi sebagai "jantung" atau repositori sentral dari seluruh aktivitas manajemen risiko. Tanpa adanya risk register yang dipelihara secara formal, output dari proses-proses yang sudah matang

seperti APO12.02 (Menganalisis Risiko) yang telah mencapai Level 3 menjadi tidak terdokumentasi dan kehilangan nilainya seiring waktu.

2) Peran APO12.04 sebagai Kanal Komunikasi Strategis: Praktik APO12.04 berfungsi sebagai "sistem saraf" yang mengalirkan informasi risiko dari tingkat operasional ke tingkat strategis. Ketika praktik ini lemah, maka informasi risiko tidak pernah sampai secara efektif kepada para pengambil keputusan, menyebabkan proses perencanaan respons (APO12.05) tidak didasarkan pada data yang komprehensif.

Dengan demikian, meskipun praktik lain telah berada di Level 2 dan 3 dan dianggap memenuhi sebagian kebutuhan, efektivitasnya menjadi terisolasi dan tidak berkelanjutan. Kegagalan pada APO12.03 dan APO12.04 memiliki dampak berantai (cascading effect) yang melemahkan keseluruhan sistem. Oleh karena itu, fokus temuan dan prioritas rekomendasi diarahkan pada kedua praktik ini bukan karena nilainya paling rendah, tetapi karena perbaikan pada kedua area ini akan memberikan dampak perbaikan yang paling signifikan dan sistemik.

4.5 Perumusan Rekomendasi Strategis

Berdasarkan hasil analisis kapabilitas yang mengidentifikasi kondisi saat ini pada Level 2 (*Managed*) dan adanya kesenjangan signifikan pada domain APO12 (*Managed Risk*), tahap berikutnya adalah merumuskan rekomendasi strategis. Rekomendasi ini dirancang untuk mengatasi paradoks kematangan yang teridentifikasi, sekaligus memperkuat fondasi tata kelola risiko teknologi informasi di Kantor DPRD Kota Sorong. Rekomendasi ini berfungsi sebagai peta jalan

(*roadmap*) yang terstruktur dan terukur untuk mengangkat kapabilitas proses secara merata.

Strategi yang diusulkan berorientasi pada penutupan kesenjangan kritis pada praktik yang masih berada di Level 1, serta melakukan standardisasi pada praktik di Level 2, dengan tujuan akhir mencapai tingkat kapabilitas target yang seragam pada Level 3 (*Established*). Fokus utama adalah pada formalisasi dokumentasi dan standardisasi komunikasi untuk menciptakan siklus manajemen risiko yang utuh dan terintegrasi. Seluruh rekomendasi ini diturunkan langsung dari temuan berbasis bukti, sehingga relevansi dan ketepatan sasarannya dapat dipertanggungjawabkan secara ilmiah.

4.5.1 Rekomendasi Peningkatan Proses APO12

Rekomendasi peningkatan proses pada domain APO12 (*Managed Risk*) disusun sebagai langkah strategis untuk menjembatani kesenjangan kapabilitas yang telah diidentifikasi sebelumnya. Penyusunan rekomendasi ini berorientasi pada pencapaian tingkat kapabilitas yang lebih tinggi, dengan menekankan pada formalisasi prosedur, standardisasi praktik, serta integrasi proses manajemen risiko ke dalam tata kelola organisasi. Dengan demikian, rekomendasi yang diajukan tidak hanya berfungsi sebagai solusi atas kelemahan yang ditemukan, tetapi juga sebagai pedoman praktis yang dapat diimplementasikan secara bertahap oleh Kantor DPRD Kota Sorong. Pada tabel 4.4 merupakan Peta jalan yang dirancang agar setiap tahapan peningkatan dapat terukur, realistis, dan selaras dengan kapasitas kelembagaan, sehingga mendukung pencapaian target kapabilitas pada Level 3 (Established).

Tabel 4.4 Peta Jalan Rekomendasi Peningkatan Proses APO12

Prioritas	Area Peningkatan (Praktik APO12)	Rekomendasi Spesifik	Penanggung Jawab	Indikator Keberhasilan
Jangka Pendek (0-6 Bulan)	APO12.03 Memelihara Profil Risiko (*Capability Level 1*)	1. Merancang dan mengesahkan template dokumen TI *Risk Register* terpusat. 2. Mengidentifikasi dan mendokumentasikan 10 risiko TI teratas sebagai pengisian awal. 3. Menetapkan Pemilik Risiko (PIC) untuk setiap risiko yang teridentifikasi.	1. Sekretaris DPRD (A) 2. Seluruh Kabag (R) 3. Tim TI (R)	1. Dokumen template TI *Risk Register* versi 1.0 disahkan. 2. Minimal 10 risiko TI telah terisi lengkap di dalam *Risk Register*.
	APO12.04 Mengartikulasikan Risiko *Capability Level 1*)	1. Menyusun draf *Standar Operasional Prosedur* (SOP) Komunikasi Risiko TI. 2. Merancang Matriks Komunikasi, Frekuensi Pelaporan, dan Template Laporan Risiko. 3. Melakukan sosialisasi awal mengenai pentingnya pelaporan risiko kepada pimpinan.	1. Sekretaris DPRD (A) 2. Kabag. Umum (R) 3. Tim TI (R)	1. Draf SOP Komunikasi Risiko TI versi 1.0 selesai disusun. 2. Matriks Komunikasi telah disetujui oleh pimpinan.

Jangka Pendek-Menengah (6-12 Bulan)	APO12.01 Mengumpulkan Data Risiko (*Capability Level 2*)	1. Menetapkan prosedur standar untuk pengumpulan data risiko dari setiap unit kerja. 2. Mengintegrasikan alur pelaporan insiden agar data otomatis masuk ke dalam draf *Risk Register*.	1. Kabag. Umum (A) 2. Seluruh Kasubag (R) 3. Tim TI (R)	1. Prosedur pengumpulan data risiko disosialisasikan 2. Minimal 80% insiden TI yang relevan tercatat sebagai input risiko.
	APO12.02 & APO12.05 (Analisis & Perencanaan) *Capability Level 3*)	1. Mengintegrasikan output dari proses analisis (APO12.02) dan perencanaan respons (APO12.05) ke dalam kolom yang sesuai di *Risk Register*.	1. Kabag. Hukum (A) 2. Kasubag. Program (R) 3. Tim TI (R)	1. Kolom "Skor Risiko" dan "Rencana Mitigasi" di Risk Register terisi secara konsisten berdasarkan hasil analisis formal.
Jangka Menengah (12-18 Bulan)	APO12.04 & APO12.03 (Komunikasi & Pemeliharaan)	1. Melaksanakan siklus pelaporan risiko triwulanan pertama sesuai SOP. 2. Melakukan rapat tinjauan risiko pertama untuk memperbarui Risk Register.	1. Sekretaris DPRD (A) 2. Seluruh Kabag (R)	1. Laporan Ringkasan Risiko TI (Periode 3 bulan pertama) terbit. 2. Notulensi rapat tinjauan risiko terdokumentasi.
	APO12.06 Menangani Risiko (*Capability Level 3*)	1. Mendokumentasikan hasil dan pembelajaran dari setiap implementasi respons risiko. 2. Menggunakan pembelajaran tersebut untuk memperbarui *Risk Register* (misalnya, mengidentifikasi	1. Kabag. Umum (A) 2. Tim TI (R)	1. Minimal ada 3 pembaruan pada Risk Register yang berasal dari pembelajaran penanganan insiden.

4.5.2 Rekomendasi 1: Implementasi *Risk Register* Terpusat untuk Mengatasi Kelemahan pada APO12

Hasil evaluasi menunjukkan bahwa praktik APO12.03 (Memelihara Profil Risiko) berada pada Level 1, yang mengindikasikan bahwa prosesnya berjalan namun tidak terkelola. Kelemahan fundamental yang teridentifikasi adalah tidak adanya sebuah artefak atau dokumen formal yang berfungsi sebagai repositori risiko terpusat. Untuk mengatasi hal ini, direkomendasikan implementasi sebuah *TI Risk Register*. Rekomendasi ini bukanlah sekadar menyarankan pembuatan daftar risiko sederhana, melainkan pembangunan sebuah dokumen terstruktur dan dinamis yang berfungsi sebagai pusat kendali untuk seluruh informasi risiko teknologi informasi. *Risk register* yang diusulkan minimal harus memuat kolom-kolom berikut untuk memastikan kelengkapan dan fungsionalitasnya:

a) ID Risiko: Kode unik untuk setiap risiko yang teridentifikasi, yang berfungsi untuk mempermudah pelacakan, referensi silang, dan audit.
b) Deskripsi Risiko: Penjelasan yang jelas dan tidak ambigu mengenai potensi kejadian risiko, mencakup penyebab dan potensi dampaknya terhadap layanan atau proses bisnis.
c) Kategori Risiko: Klasifikasi risiko ke dalam kategori yang relevan (misalnya, Teknis, Operasional, Keamanan, Kepatuhan) untuk mempermudah analisis tren dan pelaporan kepada manajemen.
d) Analisis Dampak & Tingkat Probabilitas: Penilaian kuantitatif atau kualitatif terhadap potensi kerugian (dampak) dan kemungkinan

terjadinya (probabilitas) setiap risiko, yang menjadi dasar untuk penentuan prioritas.

e) Skor Risiko: Nilai numerik yang dihitung dari dampak dan probabilitas, yang berfungsi untuk memeringkatkan risiko dari yang paling kritis hingga yang paling rendah.

f) Pemilik Risiko (PIC): Penetapan individu atau unit kerja yang secara formal bertanggung jawab untuk memantau dan memastikan bahwa risiko tersebut dikelola dengan baik.

g) Rencana Mitigasi: Deskripsi tindakan konkret dan terukur yang akan diambil untuk mengurangi dampak atau probabilitas risiko ke tingkat yang dapat diterima.

h) Status Implementasi Mitigasi: Kolom untuk memantau status terkini dari rencana mitigasi (misalnya, Belum Dimulai, Sedang Berjalan, Selesai), yang penting untuk pelaporan kemajuan.

Dengan mengimplementasikan *risk register* yang komprehensif ini, Kantor DPRD Kota Sorong akan memiliki alat manajemen yang tidak hanya mendokumentasikan risiko, tetapi juga memfasilitasi pemantauan, pengendalian, dan pelaporan secara sistematis, yang secara langsung akan meningkatkan kapabilitas proses APO12.03 dari Level 1 menuju level yang lebih matang.

4.5.3 Rekomendasi 2: Penyusunan *Standar Operasional Prosedur* (SOP) Komunikasi Risiko untuk Mengatasi Kelemahan pada APO12.04

Temuan lain yang signifikan adalah rendahnya tingkat kapabilitas praktik APO12.04 (Mengartikulasikan Risiko) yang juga berada pada Level 1. Kelemahan

utamanya adalah komunikasi risiko yang bersifat *ad-hoc*, tidak terstruktur, dan tidak terjadwal. Untuk mengatasi hal ini, direkomendasikan penyusunan sebuah *Standar Operasional Prosedur* (SOP) Komunikasi Risiko TI. Rekomendasi ini melampaui saran umum seperti "perlu meningkatkan komunikasi" dengan merinci komponen-komponen esensial yang harus ada di dalam dokumen SOP tersebut untuk memastikan efektivitasnya:

a) Tujuan dan Ruang Lingkup: Bagian yang menjelaskan secara formal fungsi dari SOP ini, batasan, serta kepada siapa saja prosedur ini berlaku, untuk menghindari ambiguitas.

b) Matriks Komunikasi: Sebuah tabel yang secara visual mendefinisikan siapa yang bertanggung jawab melaporkan, informasi apa yang harus dilaporkan, kapan harus dilaporkan, media apa yang digunakan, dan kepada siapa laporan tersebut ditujukan. Ini adalah inti dari SOP yang memastikan informasi yang tepat sampai ke orang yang tepat pada waktu yang tepat.

c) Frekuensi Pelaporan: Penetapan jadwal pelaporan yang rutin dan dapat diprediksi (misalnya, laporan ringkasan risiko disampaikan setiap triwulan kepada pimpinan, sementara laporan insiden kritis disampaikan sesegera mungkin).

d) Template Laporan Risiko: Penyediaan format laporan yang seragam dan standar. Template ini harus dirancang agar mudah dibaca dan dipahami oleh pimpinan non-teknis, dengan fokus pada dampak bisnis dan status mitigasi, bukan hanya detail teknis.

e) Mekanisme Eskalasi: Mendefinisikan alur atau prosedur formal untuk melaporkan risiko-risiko berkategori kritis yang memerlukan perhatian dan keputusan segera dari pimpinan tingkat atas, termasuk kriteria kapan sebuah risiko harus diekscalasi.

Dengan adanya SOP yang terstruktur ini, Kantor DPRD Kota Sorong akan memiliki mekanisme komunikasi yang proaktif, konsisten, dan dapat diaudit. Ini akan memastikan bahwa para pengambil keputusan memiliki informasi yang mereka butuhkan untuk mengelola risiko TI secara efektif, yang secara langsung akan meningkatkan kapabilitas proses APO12.04.

4.5.4 Perbandingan dengan Penelitian Terdahulu

Hasil penelitian ini, yang berfokus pada domain APO12 (*Managed Risk*) dalam kerangka kerja COBIT 2019, mengidentifikasi tingkat kapabilitas pada Level 2 (*Managed*) dengan adanya fenomena paradoks kematangan. Kondisi ini menunjukkan adanya kekuatan pada proses teknis (Level 3) yang tidak diimbangi oleh kelemahan fundamental pada proses dokumentasi dan komunikasi (Level 1), sehingga memerlukan intervensi strategis untuk mengintegrasikan siklus manajemen risiko secara utuh. Temuan tersebut memiliki keterkaitan sekaligus perbedaan karakteristik dibandingkan dengan hasil penelitian terdahulu yang dijadikan rujukan akademis.

Penelitian yang dilakukan oleh (Wijaya et al., 2023) menerapkan kerangka kerja COBIT 2019 pada domain APO12 untuk melakukan audit tata kelola TI di Universitas Mikroskil. Hasil penelitian tersebut juga mengidentifikasi adanya kelemahan dan risiko yang memerlukan rekomendasi perbaikan untuk

meningkatkan efisiensi dan efektivitas pengelolaan TI. Kesamaan dengan penelitian ini terletak pada penggunaan domain APO12 sebagai fokus evaluasi dan penekanan terhadap kebutuhan perbaikan proses untuk mencapai tujuan organisasi. Perbedaannya, penelitian ini mengungkap pola fragmentasi kapabilitas yang tajam di sektor legislatif daerah, di mana proses teknis sudah matang namun fondasi proseduralnya belum terbentuk. Hal ini menghasilkan rekomendasi yang lebih spesifik, yaitu implementasi Risk Register dan POS Komunikasi untuk menyambungkan kembali siklus yang terputus.

Sementara itu, penelitian yang dilakukan oleh (Howard et al., n.d.) juga mengevaluasi domain APO12 menggunakan COBIT 2019, namun pada konteks perusahaan swasta (PT Indako Trading Coy). Penelitian tersebut bertujuan membantu organisasi meningkatkan kualitas layanan dan mengurangi risiko secara umum. Walaupun menggunakan domain yang sama, pendekatan dan temuan dalam penelitian ini lebih mendalam. Penelitian ini menggunakan pendekatan berbasis bukti (evidence-based) untuk mengidentifikasi akar masalah pada ketiadaan artefak formal seperti profil risiko yang terawat dan mekanisme pelaporan yang terstruktur, sebagai penyebab utama mengapa siklus manajemen risiko tidak berjalan efektif meskipun beberapa bagiannya sudah matang.

Berdasarkan perbandingan tersebut, dapat disimpulkan bahwa penelitian ini selaras dengan tren temuan akademis terdahulu yang menunjukkan adanya ruang untuk peningkatan dalam manajemen risiko TI. Namun, penelitian ini memiliki kontribusi orisinal berupa identifikasi paradoks kematangan sebagai sebuah fenomena spesifik dalam tata kelola di sektor publik, serta perumusan peta jalan

implementasi yang terstruktur (pembuatan Risk Register dan POS Komunikasi) yang secara langsung menargetkan integrasi proses untuk membentuk siklus manajemen risiko yang utuh dan berkelanjutan.

4.6 Roadmap Implementasi Rekomendasi

Perumusan rekomendasi strategis perlu diiringi dengan sebuah peta jalan (roadmap) implementasi yang terstruktur untuk memastikan bahwa usulan perbaikan dapat diterapkan secara efektif, terukur, dan berkelanjutan oleh Kantor DPRD Kota Sorong. Implementasi rekomendasi perlu dilakukan secara bertahap untuk memastikan adopsi yang efektif. Berikut adalah tabel 4.5 Roadmap yang diusulkan, yang memprioritaskan perbaikan pada area terlemah (Level 1) terlebih dahulu, yaitu sebagai berikut:

Tabel 4.5 Roadmap Implimentasi Rekomendasi

Prioritas	Rekomendasi Utama	Penanggung Jawab	Indikator Keberhasilan
Jangka Pendek (0-6 Bulan)	**Fondasi Proses:** 1. Merancang dan mengesahkan *template* TI *Risk Register* 2. Menyusun draf SOP Komunikasi Risiko TI	**A:** Sekretaris DPRD **R:** Tim TI, Kabag. Terkait	1. Dokumen Risk Register v1.0 disahkan 2. Draf SOP Komunikasi v1.0 selesai
Jangka Menengah (6-12 Bulan)	**Standardisasi & Integrasi:** 1. Mengisi *Risk Register* dengan hasil analisis (APO12.02)	**A:** Kabag. Umum **R:** Seluruh Kabag	1. Risk Register terisi dan digunakan 2. SOP Komunikasi disosialisasikan

	2. Formalisasi dan sosialisasi SOP Komunikasi Risiko		
Jangka Panjang (12-18 Bulan)	**Perbaikan Berkelanjutan:** 1. Melaksanakan siklus pelaporan risiko (Periode 3 bulan pertama) 2. Melakukan rapat tinjauan risiko untuk memperbarui *Risk Register*.	**A:** Sekretaris DPRD **R:** Seluruh Pimpinan	1. Laporan risiko (Periode 3 bulan pertama) terbit 2. Notulensi rapat tinjauan risiko

Roadmap ini dirancang dengan pendekatan bertahap dan logis, yang bertujuan untuk membangun fondasi yang kuat sebelum beralih ke tahap yang lebih kompleks. Logika utamanya adalah memperbaiki proses yang paling lemah terlebih dahulu (Level 1), karena proses-proses ini adalah akar masalah dari siklus manajemen risiko yang terputus di Kantor DPRD Kota Sorong, yaitu sebagai berikut :

1. Fase Jangka Pendek (Fondasi Proses)

   Fase awal ini diposisikan sebagai prioritas tertinggi karena fokusnya adalah untuk membangun fondasi atau artefak dasar yang saat ini tidak ada. Berdasarkan temuan penelitian, praktik APO12.03 (Memelihara Profil Risiko) dan APO12.04 (Mengartikulasikan Risiko) berada pada tingkat kapabilitas terendah (Level 1). Kelemahan ini disebabkan oleh ketiadaan alat fundamental untuk pencatatan risiko secara terpusat (*Risk Register*) dan ketiadaan aturan formal untuk pelaporan risiko

(SOP Komunikasi). Oleh karena itu, aktivitas utama pada fase ini terkonsentrasi pada penciptaan kedua instrumen tersebut. Dengan merancang dan mengesahkan *template TI Risk Register* serta menyusun draf SOP Komunikasi, institusi akan memiliki fondasi prosedural dan dokumentasi yang sebelumnya hilang. Keberhasilan fase ini bersifat krusial, karena tanpa fondasi ini, seluruh upaya perbaikan lainnya tidak akan dapat berdiri kokoh.

2. Fase Jangkah Menengah (Standardisasi dan Integrasi)

   Setelah fondasi proses terbentuk, fase kedua berfokus pada standardisasi dan integrasi. Tujuan utama dari fase ini adalah untuk menyambungkan kembali siklus manajemen risiko yang terputus. Temuan penelitian menunjukkan bahwa beberapa proses seperti APO12.02 (Analisis Risiko) telah berjalan dengan baik dan mencapai Level 3. Namun, output dari proses yang matang tersebut tidak terdokumentasi dan terintegrasi dengan baik ke dalam siklus yang lebih besar. Aktivitas pada fase ini, seperti mengisi *Risk Register* dengan hasil analisis (APO12.02) dan memformalkan serta mensosialisasikan SOP Komunikasi, secara langsung menjembatani kesenjangan tersebut. Fase ini mengubah *Risk Register* dari sekadar template menjadi sebuah dokumen yang hidup dan fungsional, serta memastikan bahwa aturan komunikasi yang telah dirancang mulai diterapkan secara konsisten di seluruh unit kerja.

3. Fase Jangka Panjang (Perbaikan Berkelanjutan)

   Fase terakhir dirancang untuk melembagakan proses yang baru terbentuk agar menjadi sebuah siklus yang berkelanjutan dan bagian dari budaya organisasi. Setelah sistem terintegrasi dan mulai berjalan, fokusnya beralih dari pembangunan ke operasionalisasi dan pemantauan. Aktivitas utama seperti melaksanakan siklus pelaporan risiko (Periode 3 bulan pertama) sesuai dengan SOP dan mengadakan rapat tinjauan risiko untuk memperbarui *Risk Register* merupakan manifestasi dari siklus manajemen risiko yang berfungsi. Lebih lanjut, fase ini memastikan bahwa pembelajaran dari proses penanganan risiko di lapangan (APO12.06) didokumentasikan dan digunakan sebagai input untuk memperbarui profil risiko. Keberhasilan fase ini menandakan bahwa proses manajemen risiko tidak lagi bersifat statis, melainkan telah menjadi sebuah mekanisme yang hidup, adaptif, dan berkelanjutan.

4.7 Potensi Dampak dan Validasi Solusi

Bagian ini menyajikan argumentasi akhir mengenai validitas rekomendasi yang diusulkan sebagai solusi atas permasalahan yang teridentifikasi, sekaligus memproyeksikan potensi dampak positif bagi Kantor DPRD Kota Sorong jika rekomendasi tersebut diimplementasikan secara konsisten. Rangkaian rekomendasi yang telah disusun divalidasi sebagai solusi yang efektif karena secara langsung menargetkan akar permasalahan yang ditemukan pada domain APO12 (*Managed Risk*) berdasarkan analisis berbasis bukti. Misalnya, rekomendasi untuk formalisasi

pengumpulan data risiko (APO12.01) secara langsung menjawab permasalahan mendasar berupa ketiadaan prosedur dan format baku dalam pencatatan risiko. Dengan adanya kebijakan formal, SOP, dan basis data terpusat, instansi akan memiliki landasan yang jelas untuk memenuhi atribut kapabilitas Level 2 dan Level 3, seperti dokumentasi proses, standarisasi pelaksanaan, dan integrasi lintas unit.

Demikian pula, rekomendasi pada pemeliharaan profil risiko (APO12.03) dan komunikasi risiko (APO12.04) akan mengatasi kelemahan dalam pembaruan informasi risiko dan penyampaian data risiko kepada pemangku kepentingan secara sistematis. Penerapan sistem pembaruan berkala dan integrasi komunikasi risiko dalam platform informasi internal akan memperkuat koordinasi serta mempercepat respons terhadap potensi ancaman. Selanjutnya, rekomendasi terkait penentuan respons risiko (APO12.05) dan penanganan risiko (APO12.06) memberikan solusi atas belum adanya kerangka mitigasi yang baku dan prosedur respons yang terstandarisasi. Penyusunan portofolio mitigasi berbasis prioritas risiko dan pelaksanaan simulasi respons insiden secara berkala akan meningkatkan kesiapan organisasi dalam menghadapi berbagai skenario risiko, sekaligus meminimalkan potensi kerugian.

1. Implementasi rekomendasi ini secara menyeluruh berpotensi menghasilkan dampak positif yang signifikan, baik pada tataran operasional maupun strategis:
2. Dampak Operasional Peningkatan konsistensi, keandalan, dan akurasi proses manajemen risiko; penurunan jumlah insiden yang

tidak terprediksi; serta peningkatan kecepatan respons terhadap kejadian yang mengancam operasional organisasi.

3. Dampak Strategis Meningkatkan kepercayaan dan kepuasan pemangku kepentingan; mendukung pengambilan keputusan berbasis data risiko yang valid dan terkini; serta memastikan keselarasan antara kebijakan pengelolaan risiko dengan tujuan strategis DPRD Kota Sorong.
4. Dampak Kultural Mendorong transformasi budaya kerja yang proaktif dan berbasis pengelolaan risiko, di mana kesadaran dan kepatuhan terhadap prosedur menjadi bagian dari praktik kerja sehari-hari.

Dengan demikian, penerapan rekomendasi ini tidak hanya akan meningkatkan kapabilitas teknis hingga mencapai Level 3 (*Established*), tetapi juga akan memperkuat kapasitas kelembagaan DPRD Kota Sorong dalam mengelola risiko TI secara berkelanjutan, terukur, dan selaras dengan prinsip tata kelola yang baik (*good governance*).

BAB 5
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai evaluasi manajemen risiko teknologi informasi menggunakan kerangka kerja COBIT 2019 pada domain APO12 (*Managed Risk*) di Kantor DPRD Kota Sorong, penelitian ini merupakan sebuah kegiatan evaluasi yang output-nya berhenti pada tahap perumusan rekomendasi dan peta jalan (*roadmap*) implementasi. Oleh karena itu, kesimpulan yang ditarik berfokus pada hasil evaluasi kondisi saat ini (*as-is*) dan validitas rekomendasi sebagai sebuah cetak biru (*blueprint*) strategis, bukan pada pelaporan hasil dari implementasi di lapangan, berikut adalah beberapa kesimpulan utama, yaitu :

1. Tingkat kapabilitas (*capability level*) manajemen risiko TI di Kantor DPRD Kota Sorong secara keseluruhan berada pada Level 2 (*Managed*). Ini menandakan bahwa proses-proses risiko telah dikelola, namun implementasinya belum merata dan belum terintegrasi menjadi sebuah siklus yang utuh.
2. Analisis terhadap pola sebaran kapabilitas tersebut mengidentifikasi adanya fenomena paradoks kematangan. Kesenjangan terbesar (2 level) ditemukan pada praktik APO12.03 (Memelihara Profil Risiko) dan APO12.04 (Mengartikulasikan Risiko). Kelemahan fundamental pada kedua praktik ini menjadi akar masalah yang menyebabkan

3. Rekomendasi strategis yang dirumuskan untuk meningkatkan pengelolaan risiko TI secara langsung menargetkan penutupan kesenjangan yang paling kritis. Rekomendasi utama adalah:
    1. Implementasi TI *Risk Register* terpusat, sebagai solusi untuk mengatasi kelemahan pada praktik APO12.03 dengan menyediakan artefak formal untuk pencatatan, pemantauan, dan pengendalian risiko secara sistematis.
    2. Penyusunan Standar Operasional Prosedur (SOP) Komunikasi Risiko TI, sebagai solusi untuk mengatasi kelemahan pada praktik APO12.04 dengan menciptakan mekanisme pelaporan yang terstruktur, terjadwal, dan dapat diaudit.

Secara keseluruhan, penelitian ini menegaskan bahwa Kantor DPRD Kota Sorong telah memiliki fondasi yang cukup baik dalam pengelolaan risiko TI. Namun, diperlukan langkah strategis untuk meningkatkan kapabilitas menuju level yang lebih tinggi guna mendukung tata kelola yang transparan, akuntabel, dan berorientasi pada peningkatan kualitas layanan publik.

5.2 Saran

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, beberapa saran yang dapat diajukan adalah sebagai berikut:

- Saran untuk Institusi:
    1. Pihak manajemen Kantor DPRD Kota Sorong disarankan untuk menunjukkan komitmen dalam mengadopsi dan

mengimplementasikan rekomendasi yang telah diusulkan, khususnya pembuatan *Risk Register* dan SOP Komunikasi Risiko, sebagai langkah awal untuk membangun fondasi manajemen risiko TI yang solid.

2. Setelah rekomendasi diimplementasikan, disarankan untuk melakukan evaluasi ulang tingkat kapabilitas secara berkala (misalnya setiap satu atau dua tahun) untuk mengukur efektivitas dari inisiatif perbaikan yang telah dilakukan dan memastikan adanya siklus perbaikan yang berkelanjutan.

- Saran untuk Penelitian Selanjutnya:
  1. Penelitian ini hanya berfokus pada domain APO12 (*Managed Risk*). Penelitian selanjutnya dapat diperluas dengan mengevaluasi domain-domain lain dalam kerangka kerja COBIT 2019 yang juga relevan dengan konteks institusi, seperti domain DSS (*Deliver, Service, and Support*) untuk mengukur kualitas layanan TI.
  2. Temuan mengenai adanya kesenjangan antara kematangan proses teknis (Level 3) dengan proses administratif (Level 1) merupakan sebuah fenomena yang menarik. Penelitian selanjutnya dapat melakukan studi komparatif di beberapa instansi pemerintah sejenis untuk menguji apakah fenomena "siklus yang terputus" ini merupakan sebuah pola umum dalam tata kelola TI di sektor publik.

3. Penelitian ini berhenti pada tahap perumusan rekomendasi. Penelitian selanjutnya dapat berfokus pada tahap implementasi dari rekomendasi yang diajukan, kemudian mengukur dampak dari implementasi tersebut terhadap peningkatan tingkat kapabilitas manajemen risiko TI di institusi.

DAFTAR PUSTAKA

[1] H. Heriyanto, "Urgensi Penerapan E-Government Dalam Pelayanan Publik," *Musamus Journal of Public Administration*, vol. 4, no. 2, 2022, doi: 10.35724/mjpa.v4i2.4128.

[2] J. Hutahaean, J. Efendi Hutagalung, and C. Maulana, "Peningkatan Efektivitas Pelayanan Melalui Pemanfaatan Teknologi Informasi di Kantor DPRD Tanjungbalai," *Jurnal Bangun Abdimas*, vol. 3, no. 1, pp. 240–244, May 2024, doi: 10.56854/ba.v3i1.334.

[3] S. T. A. Ramadhani and R. Andriani, "Evaluasi Manajemen Risiko Layanan Perpustakaan Menggunakan Kerangka Kerja Cobit 5," *JURNAL TECNOSCIENZA*, vol. 5, no. 2, 2021, doi: 10.51158/tecnoscienza.v5i2.407.

[4] F. Mulianingsih, "Manajemen Risiko Digital: Strategi Keamanan Siber untuk Mitigasi Ancaman di Era Revolusi Industri 4.0," 2025.

[5] D. Solak and M. Topaloglu, "The Perception Analysis of Cyber Crimes in View of Computer Science Students," *Procedia Soc Behav Sci*, vol. 182, pp. 590–595, May 2015, doi: 10.1016/j.sbspro.2015.04.787.

[6] R. Anugrah, E. Utami, and A. H. Muhammad, "Analisis Manajemen Risiko TI Pada Perguruan Tinggi XYZ Berbasis COBIT 2019 Dengan Pertimbangan Domain APO12," *Jurnal Ilmiah Universitas Batanghari Jambi*, vol. 22, no. 2, 2022, doi: 10.33087/jiubj.v22i2.2175.

[7] A. Della Ariesta and A. Reza Perdanakusuma, "Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. MyECO Teknologi Nusantara menggunakan Framework COBIT 2019 Proses EDM03 dan APO12," *... Teknologi Informasi dan ...*, vol. 6, no. 12, 2022.

[8] K. Irawan, B. T. Hanggara, and Suprapto, "Tampilan Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi menggunakan Framework COBIT 2019 proses EDM03 dan APO12 (Studi Kasus pada PT Bank BRI

Unit Bangorejo)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komput*, vol. 7, 2023.

[9] G. M. W. Tangka, C. Lumingkewas, and E. Lompoliu, "IT Governance Maturity Assessment at PT PLN Suluttengo Using COBIT 2019," *International Journal of Engineering, Science and Information Technology*, vol. 5, no. 2, pp. 195–203, Feb. 2025, doi: 10.52088/ijesty.v5i2.811.

[10] K. Leonardo and R. Latuperissa, "Information Technology Governance Design in Trading Companies Using the COBIT 2019 Framework," *Journal of Information Systems and Informatics*, vol. 6, no. 3, pp. 1466–1483, Sep. 2024, doi: 10.51519/journalisi.v6i3.798.

[11] A. Zaini, A. P. Widodo, and D. M. K. Nugraheni, "Information System Governance Evaluation at Diskominfo Central Java Using COBIT 2019 Framework," *Scientific Journal of Informatics*, vol. 12, no. 1, pp. 67–76, May 2025, doi: 10.15294/sji.v12i1.22883.

[12] S. Howard, T. Wijaya, R. Yunis, and M. -, "Evaluasi Tata Kelola Teknologi Informasi Pada PT Indako Trading Coy Dengan Menggunakan Framework COBIT 2019 Domain APO12," *Jurnal SIFO Mikroskil*, vol. 24, no. 2, 2023, doi: 10.55601/jsm.v24i2.1030.

[13] D. P. Utama, A. H. Muhammad, and A. Purwanto, "AUDIT MANAJEMEN MASALAH TEKNOLOGI INFORMASI MENGGUNAKAN KERANGKA KERJA COBIT 2019 DOMAIN DSS03," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 8, no. 3, pp. 839–846, Aug. 2023, doi: 10.29100/jipi.v8i3.3946.

[14] C. Wijaya, M. Sukamto, R. Yunis, and M. Megawati, "Audit Tata Kelola TI Menggunakan COBIT 2019 Domain APO-12 Pada Universitas Mikroskil," *Jurnal SIFO Mikroskil*, vol. 24, no. 2, 2023, doi: 10.55601/jsm.v24i2.1025.

[15] Muh Wal Ikram, W. W. Winarno, and M. R. Arief, "PERENCANAAN AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019 (STUDI KASUS: PT. LAZ COAL MANDIRI)," *TEKNIMEDIA: Teknologi Informasi dan Multimedia*, vol. 4, no. 2, 2023, doi: 10.46764/teknimedia.v4i2.109.

[16] I. G. Wikan Aditya, I. G. Putu Krisna Juliharta, and I. G. Agung Pramesti Dwi Putri, "PENERAPAN FRAMEWORK COBIT 2019 DALAM AUDIT TATA KELOLA SISTEM INFORMASI PADA LPD DESA BERABAN," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, no. 4, 2024, doi: 10.36040/jati.v7i4.7142.

[17] M. M. Asep Deni, *Manajemen Risiko Pada Era Digital*. CV Rey Media Grafika, 2024.

[18] M. Silvianthie and A. Reza Perdanakusuma, "Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. IKI Karunia Indonesia menggunakan COBIT 2019," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 12, 2022.

[19] ISACA, *COBIT 2019 : Governance and Management Objectives*. 2019.

[20] E. Amore, T. Dilger, C. Ploder, R. Bernsteiner, and M. Mezzenzana, "Leverage the COBIT 2019 Design Toolkit in an SME Context: A Multiple Case Study," *KnE Social Sciences*, 2023, doi: 10.18502/kss.v8i1.12636.

LAMPIRAN

Lampiran 1 Foto-Foto Bersama Pegawai Kantor DPRD Kota Sorong

Lampiran 2 Kuesioner 1 - 5 Kantor DPRD Kota Sorong

KUESIONER PENILAIAN KAPABILITAS DOMAIN APO12 (MANAGE RISK)

Nama Peneliti	Fajar Maulana Ahsan Abbas
NIM	23.51.2492
Prodi	Magister Informatika, Universitas AMIKOM Yogyakarta
Judul Penelitian	Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: Kantor DPRD Kota Sorong)

Tujuan Kuesioner: Kuesioner ini bertujuan untuk menilai tingkat kapabilitas (capability level) proses manajemen Risiko TI di Kantor DPRD Kota Sorong, berdasarkan domain APO12 dari kerangka kerja COBIT 2019.

Petunjuk Pengisian: Untuk setiap pertanyaan, mohon berikan peringkat pencapaian berdasarkan kondisi saat ini di institusi Anda. Peringkat harus didasarkan pada bukti yang ada (dokumen kebijakan, SOP, notulensi rapat, laporan, hasil survei, dll.), bukan hanya asumsi.

Skala Peringkat Penilaian:

Peringkat	Nama	Persentase Pencapaian	Deskripsi
N	Not Achieved	0 - 15%	Sangat sedikit atau tidak ada bukti sama sekali bahwa aktivitas ini dilaksanakan.
P	Partially Achieved	>15% - 50%	Ada beberapa bukti bahwa aktivitas ini dilaksanakan, namun masih terdapat kelemahan yang signifikan.
L	Largely Achieved	>50% - 85%	Ada bukti yang kuat bahwa aktivitas ini dilaksanakan secara efektif, meskipun masih ada kelemahan minor.
F	Fully Achieved	>85% - 100%	Ada bukti yang lengkap dan kuat bahwa aktivitas ini dilaksanakan secara konsisten dan mencapai tujuannya.

IDENTITAS RESPONDEN	
Nama Responden	**Regina AP, SH., MM**
NIP/NIDN	
Unit Kerja	
Jabatan	**Kasubag. Program Dan Keuangan**

Tanggal Pengisian	8 April 2025

Praktik 1: APO12.01 Mengumpulkan Data Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengidentifikasi dan mengumpulkan data yang relevan untuk membantu mengidentifikasi peristiwa risiko TI di masa lalu dan masa depan.	F	*Fully Achieved*	Prosesnya berjalan, saya tahu ada pengumpulan data risiko.
Level 2 (Managed)	2.1 Proses pengumpulan data risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	L	*Largely Achieved*	Dikelola secara dasar, terlihat dari beberapa notulensi rapat.
	2.2 Output dari proses pengumpulan data (misalnya daftar sumber risiko) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Dikelola secara dasar, terlihat dari beberapa notulensi rapat.
Level 3 (Established)	3.1 Proses pengumpulan data risiko telah terdefinisi dengan baik dan terstandarisasi di seluruh institusi.	P	*Partially Achieved*	Belum jadi standar, tidak ada SOP yang disahkan.

Praktik 2: APO12.02 Menganalisis Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menganalisis relevansi dan signifikansi dari peristiwa risiko yang telah teridentifikasi.	F	*Fully Achieved*	Analisis risiko sudah pasti dilakukan
Level 2 (Managed)	2.1 Proses analisis risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	F	*Fully Achieved*	Prosesnya terkelola baik, saya menerima laporan prioritas risiko
	2.2 Output dari proses analisis (misalnya laporan prioritas risiko) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Prosesnya terkelola baik, saya menerima laporan prioritas risiko
Level 3 (Established)	3.1 Proses analisis risiko telah terdefinisi dengan baik dan terstandarisasi menggunakan metodologi formal.	F	*Fully Achieved*	Sudah jadi standar, kami punya dokumen metodologi analisis formal.

Praktik 3: APO12.03 Memelihara Profil Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi memelihara inventaris (daftar) risiko dan atributnya (misalnya, dampak, probabilitas, pemilik).	L	*Largely Achieved*	Ada pendataan risiko, tapi informal.
Level 2 (Managed)	2.1 Proses pemeliharaan profil risiko (risk register) direncanakan, dipantau, dan disesuaikan.	N	*Not Achieved*	Belum dikelola, saya tidak pernah lihat dokumen *risk register* formal.
	2.2 Output dari proses (profil risiko yang diperbarui) ditetapkan, dikendalikan, dan dipelihara secara rutin.	P	*Partially Achieved*	Belum dikelola, saya tidak pernah lihat dokumen *risk register* formal.
Level 3 (Established)	3.1 Proses pemeliharaan profil risiko telah terdefinisi dengan baik dan terintegrasi dengan proses lain.	N	*Not Achieved*	Belum jadi standar karena belum dikelola sama sekali.

Praktik 4: APO12.04 Mengartikulasikan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengkomunikasikan informasi risiko kepada para pemangku kepentingan.	L	*Largely Achieved*	Komunikasi hanya terjadi jika ada insiden kritis.
Level 2 (Managed)	2.1 Proses komunikasi risiko direncanakan dan memiliki jadwal pelaporan yang jelas.	P	*Partially Achieved*	Belum dikelola, tidak ada jadwal pelaporan rutin.
	2.2 Output dari proses (misalnya laporan risiko) memiliki format yang ditetapkan dan dikendalikan.	N	*Not Achieved*	Belum dikelola, tidak ada jadwal pelaporan rutin.
Level 3 (Established)	3.1 Proses komunikasi risiko telah terdefinisi dengan baik dan terstandarisasi.	N	*Not Achieved*	Belum jadi standar, tidak ada SOP Komunikasi Risiko.

Praktik 5: APO12.05 Merencanakan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengelola risiko dengan merencanakan tindakan respons (misalnya mitigasi, transfer, penerimaan).	F	*Fully Achieved*	Perencanaan respons risiko pasti dilakukan.
Level 2 (Managed)	2.1 Proses perencanaan respons risiko direncanakan, dipantau, dan disesuaikan.	F	*Fully Achieved*	Terkelola baik, saya menyetujui dokumen Rencana Mitigasi.
	2.2 Output dari proses (dokumen rencana mitigasi) ditetapkan, dikendalikan, dan dipelihara.	F	*Fully Achieved*	Terkelola baik, saya menyetujui dokumen Rencana Mitigasi.
Level 3 (Established)	3.1 Proses perencanaan respons risiko telah terdefinisi dengan baik dan terstandarisasi.	L	*Largely Achieved*	Sudah jadi standar, didukung notulensi rapat pembahasan.

Praktik 6: APO12.06 MengImplementasikan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menerapkan tindakan respons risiko yang telah direncanakan.	F	*Fully Achieved*	Implementasi sudah pasti dijalankan.
Level 2 (Managed)	2.1 Proses implementasi respons risiko direncanakan, dipantau, dan disesuaikan.	L	*Largely Achieved*	Terkelola baik, saya menerima laporan hasil implementasi.
	2.2 Output dari proses (laporan implementasi) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Terkelola baik, saya menerima laporan hasil implementasi.
Level 3 (Established)	3.1 Proses implementasi respons risiko telah terdefinisi dengan baik dan terstandarisasi.	F	*Fully Achieved*	Sudah jadi standar, proses eksekusi dan pelaporan sudah mapan.

KUESIONER PENILAIAN KAPABILITAS DOMAIN APO12 (MANAGE RISK)

Nama Peneliti	Fajar Maulana Ahsan Abbas
NIM	23.51.2492
Prodi	Magister Informatika, Universitas AMIKOM Yogyakarta
Judul Penelitian	Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: Kantor DPRD Kota Sorong)

Tujuan Kuesioner: Kuesioner ini bertujuan untuk menilai tingkat kapabilitas (capability level) proses manajemen Risiko TI di Kantor DPRD Kota Sorong, berdasarkan domain APO12 dari kerangka kerja COBIT 2019.

Petunjuk Pengisian: Untuk setiap pertanyaan, mohon berikan peringkat pencapaian berdasarkan kondisi saat ini di institusi Anda. Peringkat harus didasarkan pada bukti yang ada (dokumen kebijakan, SOP, notulensi rapat, laporan, hasil survei, dll.), bukan hanya asumsi.

Skala Peringkat Penilaian:

Peringkat	Nama	Persentase Pencapaian	Deskripsi
N	Not Achieved	0 - 15%	Sangat sedikit atau tidak ada bukti sama sekali bahwa aktivitas ini dilaksanakan.
P	Partially Achieved	>15% - 50%	Ada beberapa bukti bahwa aktivitas ini dilaksanakan, namun masih terdapat kelemahan yang signifikan.
L	Largely Achieved	>50% - 85%	Ada bukti yang kuat bahwa aktivitas ini dilaksanakan secara efektif, meskipun masih ada kelemahan minor.
F	Fully Achieved	>85% - 100%	Ada bukti yang lengkap dan kuat bahwa aktivitas ini dilaksanakan secara konsisten dan mencapai tujuannya.

IDENTITAS RESPONDEN	
Nama Responden	**Gotlief Runpaisum, SE**
NIP/NIDN	
Unit Kerja	**Setwan Kota Sorong**
Jabatan	**Kasubag. Pprogram Dan Keuangan**

Tanggal Pengisian	8 April 2025

Praktik 1: APO12.01 Mengumpulkan Data Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengidentifikasi dan mengumpulkan data yang relevan untuk membantu mengidentifikasi peristiwa risiko TI di masa lalu dan masa depan.	F	*Fully Achieved*	Saya terlibat pengumpulan data terkait keuangan.
Level 2 (Managed)	2.1 Proses pengumpulan data risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	L	*Largely Achieved*	Ada perencanaan informal, terlihat dari notulensi rapat.
	2.2 Output dari proses pengumpulan data (misalnya daftar sumber risiko) ditetapkan, dikendalikan, dan dipelihara.	P	*Partially Achieved*	Ada perencanaan informal, terlihat dari notulensi rapat.
Level 3 (Established)	3.1 Proses pengumpulan data risiko telah terdefinisi dengan baik dan terstandarisasi di seluruh institusi.	N	*Not Achieved*	Belum jadi standar, tidak ada SOP yang jadi acuan.

Praktik 2: APO12.02 Menganalisis Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menganalisis relevansi dan signifikansi dari peristiwa risiko yang telah teridentifikasi.	F	*Fully Achieved*	Proses analisis risiko sudah pasti dilaksanakan.
Level 2 (Managed)	2.1 Proses analisis risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	F	*Fully Achieved*	Terkelola baik, saya menggunakan laporan hasil analisis untuk anggaran.
	2.2 Output dari proses analisis (misalnya laporan prioritas risiko) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Terkelola baik, saya menggunakan laporan hasil analisis untuk anggaran.
Level 3 (Established)	3.1 Proses analisis risiko telah terdefinisi dengan baik dan terstandarisasi menggunakan metodologi formal.	F	*Fully Achieved*	Sudah jadi standar, kami punya dokumen metodologi yang jelas.

Praktik 3: APO12.03 Memelihara Profil Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi memelihara inventaris (daftar) risiko dan atributnya (misalnya, dampak, probabilitas, pemilik).	P	*Partially Achieved*	Ada pendataan risiko, tapi tidak lengkap.
Level 2 (Managed)	2.1 Proses pemeliharaan profil risiko (risk register) direncanakan, dipantau, dan disesuaikan.	N	*Not Achieved*	Belum dikelola, tidak ada *risk register* formal untuk acuan program.
	2.2 Output dari proses (profil risiko yang diperbarui) ditetapkan, dikendalikan, dan dipelihara secara rutin.	N	*Not Achieved*	Belum dikelola, tidak ada *risk register* formal untuk acuan program.
Level 3 (Established)	3.1 Proses pemeliharaan profil risiko telah terdefinisi dengan baik dan terintegrasi dengan proses lain.	N	*Not Achieved*	Belum jadi standar sama sekali.

Praktik 4: APO12.04 Mengartikulasikan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengkomunikasikan informasi risiko kepada para pemangku kepentingan.	L	*Largely Achieved*	Komunikasi hanya sebatas lisan atau email.
Level 2 (Managed)	2.1 Proses komunikasi risiko direncanakan dan memiliki jadwal pelaporan yang jelas.	N	*Not Achieved*	Belum dikelola, tidak ada jadwal atau format laporan yang saya terima.
	2.2 Output dari proses (misalnya laporan risiko) memiliki format yang ditetapkan dan dikendalikan.	P	*Partially Achieved*	Belum dikelola, tidak ada jadwal atau format laporan yang saya terima.
Level 3 (Established)	3.1 Proses komunikasi risiko telah terdefinisi dengan baik dan terstandarisasi.	N	*Not Achieved*	Belum ada SOP Komunikasi Risiko.

Praktik 5: APO12.05 Merencanakan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengelola risiko dengan merencanakan tindakan respons (misalnya mitigasi, transfer, penerimaan).	F	*Fully Achieved*	Perencanaan respons pasti dilakukan
Level 2 (Managed)	2.1 Proses perencanaan respons risiko direncanakan, dipantau, dan disesuaikan.	L	*Largely Achieved*	Terkelola baik, saya terlibat penyusunan dokumen Rencana Mitigasi.
	2.2 Output dari proses (dokumen rencana mitigasi) ditetapkan, dikendalikan, dan dipelihara.	F	*Fully Achieved*	Terkelola baik, saya terlibat penyusunan dokumen Rencana Mitigasi.
Level 3 (Established)	3.1 Proses perencanaan respons risiko telah terdefinisi dengan baik dan terstandarisasi.	F	*Fully Achieved*	Sudah jadi standar, didukung notulensi rapat pembahasan anggaran.

Praktik 6: APO12.06 MengImplementasikan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menerapkan tindakan respons risiko yang telah direncanakan.	F	*Fully Achieved*	Implementasi pasti berjalan.
Level 2 (Managed)	2.1 Proses implementasi respons risiko direncanakan, dipantau, dan disesuaikan.	F	*Fully Achieved*	Terkelola baik, saya menerima laporan implementasi untuk keuangan.
	2.2 Output dari proses (laporan implementasi) ditetapkan, dikendalikan, dan dipelihara.	F	*Fully Achieved*	Terkelola baik, saya menerima laporan implementasi untuk keuangan.
Level 3 (Established)	3.1 Proses implementasi respons risiko telah terdefinisi dengan baik dan terstandarisasi.	L	*Largely Achieved*	Sudah jadi standar, prosesnya sudah mapan.

KUESIONER PENILAIAN KAPABILITAS DOMAIN APO12 (MANAGE RISK)

Nama Peneliti	Fajar Maulana Ahsan Abbas
NIM	23.51.2492
Prodi	Magister Informatika, Universitas AMIKOM Yogyakarta
Judul Penelitian	Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: Kantor DPRD Kota Sorong)

Tujuan Kuesioner: Kuesioner ini bertujuan untuk menilai tingkat kapabilitas (capability level) proses manajemen Risiko TI di Kantor DPRD Kota Sorong, berdasarkan domain APO12 dari kerangka kerja COBIT 2019.

Petunjuk Pengisian: Untuk setiap pertanyaan, mohon berikan peringkat pencapaian berdasarkan kondisi saat ini di institusi Anda. Peringkat harus didasarkan pada bukti yang ada (dokumen kebijakan, SOP, notulensi rapat, laporan, hasil survei, dll.), bukan hanya asumsi.

Skala Peringkat Penilaian:

Peringkat	Nama	Persentase Pencapaian	Deskripsi
N	Not Achieved	0 - 15%	Sangat sedikit atau tidak ada bukti sama sekali bahwa aktivitas ini dilaksanakan.
P	Partially Achieved	>15% - 50%	Ada beberapa bukti bahwa aktivitas ini dilaksanakan, namun masih terdapat kelemahan yang signifikan.
L	Largely Achieved	>50% - 85%	Ada bukti yang kuat bahwa aktivitas ini dilaksanakan secara efektif, meskipun masih ada kelemahan minor.
F	Fully Achieved	>85% - 100%	Ada bukti yang lengkap dan kuat bahwa aktivitas ini dilaksanakan secara konsisten dan mencapai tujuannya.

IDENTITAS RESPONDEN	
Nama Responden	
NIP/NIDN	
Unit Kerja	**Sekretariat DPR Kota Sorong**
Jabatan	**Kasubang. Persidangan**

Tanggal Pengisian	8 April 2025

Praktik 1: APO12.01 Mengumpulkan Data Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengidentifikasi dan mengumpulkan data yang relevan untuk membantu mengidentifikasi peristiwa risiko TI di masa lalu dan masa depan.	F	*Fully Achieved*	Prosesnya berjalan, saya sering lapor potensi risiko persidangan.
Level 2 (Managed)	2.1 Proses pengumpulan data risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	P	*Partially Achieved*	Tidak terencana, pengumpulan data hanya jika ada laporan insiden.
	2.2 Output dari proses pengumpulan data (misalnya daftar sumber risiko) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Tidak terencana, pengumpulan data hanya jika ada laporan insiden.
Level 3 (Established)	3.1 Proses pengumpulan data risiko telah terdefinisi dengan baik dan terstandarisasi di seluruh institusi.	P	*Partially Achieved*	Belum jadi standar, tidak ada SOP untuk pengumpulan data.

Praktik 2: APO12.02 Menganalisis Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menganalisis relevansi dan signifikansi dari peristiwa risiko yang telah teridentifikasi.	F	*Fully Achieved*	Analisis risiko pasti dilakukan.
Level 2 (Managed)	2.1 Proses analisis risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	L	*Largely Achieved*	Terkelola baik, saya lihat laporan analisis untuk pengadaan alat sidang.
	2.2 Output dari proses analisis (misalnya laporan prioritas risiko) ditetapkan, dikendalikan, dan dipelihara.	F	*Fully Achieved*	Terkelola baik, saya lihat laporan analisis untuk pengadaan alat sidang.
Level 3 (Established)	3.1 Proses analisis risiko telah terdefinisi dengan baik dan terstandarisasi menggunakan metodologi formal.	L	*Largely Achieved*	Sudah jadi standar, tim TI pakai dokumen metodologi yang konsisten.

Praktik 3: APO12.03 Memelihara Profil Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi memelihara inventaris (daftar) risiko dan atributnya (misalnya, dampak, probabilitas, pemilik).	L	*Largely Achieved*	Ada pendataan risiko, tapi saya tak pernah lihat bentuknya.
Level 2 (Managed)	2.1 Proses pemeliharaan profil risiko (risk register) direncanakan, dipantau, dan disesuaikan.	P	*Partially Achieved*	Belum dikelola, tidak ada *risk register* yang disosialisasikan.
	2.2 Output dari proses (profil risiko yang diperbarui) ditetapkan, dikendalikan, dan dipelihara secara rutin.	N	*Not Achieved*	Belum dikelola, tidak ada *risk register* yang disosialisasikan.
Level 3 (Established)	3.1 Proses pemeliharaan profil risiko telah terdefinisi dengan baik dan terintegrasi dengan proses lain.	N	*Not Achieved*	Belum jadi standar institusi.

Praktik 4: APO12.04 Mengartikulasikan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengkomunikasikan informasi risiko kepada para pemangku kepentingan.	P	*Partially Achieved*	Komunikasi risiko hanya secara lisan.
Level 2 (Managed)	2.1 Proses komunikasi risiko direncanakan dan memiliki jadwal pelaporan yang jelas.	N	*Not Achieved*	Tidak ada jadwal atau format laporan.
	2.2 Output dari proses (misalnya laporan risiko) memiliki format yang ditetapkan dan dikendalikan.	N	*Not Achieved*	Tidak ada jadwal atau format laporan.
Level 3 (Established)	3.1 Proses komunikasi risiko telah terdefinisi dengan baik dan terstandarisasi.	N	*Not Achieved*	Tidak ada SOP komunikasi risiko.

Praktik 5: APO12.05 Merencanakan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengelola risiko dengan merencanakan tindakan respons (misalnya mitigasi, transfer, penerimaan).	F	*Fully Achieved*	Perencanaan respons pasti dilakukan.
Level 2 (Managed)	2.1 Proses perencanaan respons risiko direncanakan, dipantau, dan disesuaikan.	F	*Fully Achieved*	Terkelola baik, saya dilibatkan dalam pembahasan dokumen Rencana Mitigasi.
	2.2 Output dari proses (dokumen rencana mitigasi) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Terkelola baik, saya dilibatkan dalam pembahasan dokumen Rencana Mitigasi.
Level 3 (Established)	3.1 Proses perencanaan respons risiko telah terdefinisi dengan baik dan terstandarisasi.	F	*Fully Achieved*	Sudah jadi standar, dibuktikan dengan notulensi rapat rutin.

Praktik 6: APO12.06 MengImplementasikan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menerapkan tindakan respons risiko yang telah direncanakan.	F	*Fully Achieved*	Implementasi perbaikan pasti berjalan.
Level 2 (Managed)	2.1 Proses implementasi respons risiko direncanakan, dipantau, dan disesuaikan.	F	*Fully Achieved*	Terkelola baik, saya menerima laporan implementasi setelahnya.
	2.2 Output dari proses (laporan implementasi) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Terkelola baik, saya menerima laporan implementasi setelahnya.
Level 3 (Established)	3.1 Proses implementasi respons risiko telah terdefinisi dengan baik dan terstandarisasi.	L	*Largely Achieved*	Sudah jadi standar, hasilnya kami rasakan langsung.

KUESIONER PENILAIAN KAPABILITAS DOMAIN APO12 (MANAGE RISK)

Nama Peneliti	Fajar Maulana Ahsan Abbas
NIM	23.51.2492
Prodi	Magister Informatika, Universitas AMIKOM Yogyakarta
Judul Penelitian	Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: Kantor DPRD Kota Sorong)

Tujuan Kuesioner: Kuesioner ini bertujuan untuk menilai tingkat kapabilitas (capability level) proses manajemen Risiko TI di Kantor DPRD Kota Sorong, berdasarkan domain APO12 dari kerangka kerja COBIT 2019.

Petunjuk Pengisian: Untuk setiap pertanyaan, mohon berikan peringkat pencapaian berdasarkan kondisi saat ini di institusi Anda. Peringkat harus didasarkan pada bukti yang ada (dokumen kebijakan, SOP, notulensi rapat, laporan, hasil survei, dll.), bukan hanya asumsi.

Skala Peringkat Penilaian:

Peringkat	Nama	Persentase Pencapaian	Deskripsi
N	Not Achieved	0 - 15%	Sangat sedikit atau tidak ada bukti sama sekali bahwa aktivitas ini dilaksanakan.
P	Partially Achieved	>15% - 50%	Ada beberapa bukti bahwa aktivitas ini dilaksanakan, namun masih terdapat kelemahan yang signifikan.
L	Largely Achieved	>50% - 85%	Ada bukti yang kuat bahwa aktivitas ini dilaksanakan secara efektif, meskipun masih ada kelemahan minor.
F	Fully Achieved	>85% - 100%	Ada bukti yang lengkap dan kuat bahwa aktivitas ini dilaksanakan secara konsisten dan mencapai tujuannya.

IDENTITAS RESPONDEN	
Nama Responden	**Fatmawati Djalali, S.IP., MM**
NIP/NIDN	
Unit Kerja	**Setwan Kota Sorong**
Jabatan	**Kabag. Keuangan**

Tanggal Pengisian	8 April 2025

Praktik 1: APO12.01 Mengumpulkan Data Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengidentifikasi dan mengumpulkan data yang relevan untuk membantu mengidentifikasi peristiwa risiko TI di masa lalu dan masa depan.	F	*Fully Achieved*	Proses berjalan, saya kadang dimintai data finansial.
Level 2 (Managed)	2.1 Proses pengumpulan data risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	L	*Largely Achieved*	Tidak terencana, permintaan data bersifat insidental.
	2.2 Output dari proses pengumpulan data (misalnya daftar sumber risiko) ditetapkan, dikendalikan, dan dipelihara.	P	*Partially Achieved*	Tidak terencana, permintaan data bersifat insidental.
Level 3 (Established)	3.1 Proses pengumpulan data risiko telah terdefinisi dengan baik dan terstandarisasi di seluruh institusi.	N	*Not Achieved*	Belum jadi standar, tidak ada SOP yang mengatur.

Praktik 2: APO12.02 Menganalisis Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menganalisis relevansi dan signifikansi dari peristiwa risiko yang telah teridentifikasi.	F	*Fully Achieved*	Analisis risiko pasti dilakukan.
Level 2 (Managed)	2.1 Proses analisis risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	F	*Fully Achieved*	Terkelola baik, saya menerima laporan hasil analisis untuk pengajuan anggaran.
	2.2 Output dari proses analisis (misalnya laporan prioritas risiko) ditetapkan, dikendalikan, dan dipelihara.	F	*Fully Achieved*	Terkelola baik, saya menerima laporan hasil analisis untuk pengajuan anggaran.
Level 3 (Established)	3.1 Proses analisis risiko telah terdefinisi dengan baik dan terstandarisasi menggunakan metodologi formal.	L	*Largely Achieved*	Sudah jadi standar, saya tahu ada dokumen metodologi yang dipakai.

Praktik 3: APO12.03 Memelihara Profil Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi memelihara inventaris (daftar) risiko dan atributnya (misalnya, dampak, probabilitas, pemilik).	L	*Largely Achieved*	Mungkin ada, tapi saya tidak pernah melihatnya.
Level 2 (Managed)	2.1 Proses pemeliharaan profil risiko (risk register) direncanakan, dipantau, dan disesuaikan.	N	*Not Achieved*	Belum dikelola, tidak ada *risk register* sebagai acuan anggaran.
	2.2 Output dari proses (profil risiko yang diperbarui) ditetapkan, dikendalikan, dan dipelihara secara rutin.	P	*Partially Achieved*	Belum dikelola, tidak ada *risk register* sebagai acuan anggaran.
Level 3 (Established)	3.1 Proses pemeliharaan profil risiko telah terdefinisi dengan baik dan terintegrasi dengan proses lain.	N	*Not Achieved*	Belum jadi standar institusi.

Praktik 4: APO12.04 Mengartikulasikan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengkomunikasikan informasi risiko kepada para pemangku kepentingan.	L	*Largely Achieved*	Komunikasi hanya lisan jika terkait keuangan.
Level 2 (Managed)	2.1 Proses komunikasi risiko direncanakan dan memiliki jadwal pelaporan yang jelas.	P	*Partially Achieved*	Belum dikelola, tidak ada jadwal atau format laporan yang standar.
	2.2 Output dari proses (misalnya laporan risiko) memiliki format yang ditetapkan dan dikendalikan.	N	*Not Achieved*	Belum dikelola, tidak ada jadwal atau format laporan yang standar.
Level 3 (Established)	3.1 Proses komunikasi risiko telah terdefinisi dengan baik dan terstandarisasi.	N	*Not Achieved*	Belum ada SOP Komunikasi Risiko.

Praktik 5: APO12.05 Merencanakan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengelola risiko dengan merencanakan tindakan respons (misalnya mitigasi, transfer, penerimaan).	F	*Fully Achieved*	Perencanaan respons pasti dilakukan.
Level 2 (Managed)	2.1 Proses perencanaan respons risiko direncanakan, dipantau, dan disesuaikan.	F	*Fully Achieved*	Terkelola baik, saya dilibatkan dalam pembahasan dokumen Rencana Mitigasi.
	2.2 Output dari proses (dokumen rencana mitigasi) ditetapkan, dikendalikan, dan dipelihara.	F	*Fully Achieved*	Terkelola baik, saya dilibatkan dalam pembahasan dokumen Rencana Mitigasi.
Level 3 (Established)	3.1 Proses perencanaan respons risiko telah terdefinisi dengan baik dan terstandarisasi.	L	*Largely Achieved*	Sudah jadi standar, dibuktikan dengan notulensi rapat yang saya ikuti.

Praktik 6: APO12.06 MengImplementasikan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menerapkan tindakan respons risiko yang telah direncanakan.	F	*Fully Achieved*	Implementasi pasti berjalan.
Level 2 (Managed)	2.1 Proses implementasi respons risiko direncanakan, dipantau, dan disesuaikan.	L	*Largely Achieved*	Terkelola baik, saya menerima laporan implementasi dan realisasi anggaran.
	2.2 Output dari proses (laporan implementasi) ditetapkan, dikendalikan, dan dipelihara.	F	*Fully Achieved*	Terkelola baik, saya menerima laporan implementasi dan realisasi anggaran.
Level 3 (Established)	3.1 Proses implementasi respons risiko telah terdefinisi dengan baik dan terstandarisasi.	F	*Fully Achieved*	Sudah jadi standar dan prosesnya mapan.

KUESIONER PENILAIAN KAPABILITAS DOMAIN APO12 (MANAGE RISK)

Nama Peneliti	Fajar Maulana Ahsan Abbas
NIM	23.51.2492
Prodi	Magister Informatika, Universitas AMIKOM Yogyakarta
Judul Penelitian	Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: Kantor DPRD Kota Sorong)

Tujuan Kuesioner: Kuesioner ini bertujuan untuk menilai tingkat kapabilitas (capability level) proses manajemen Risiko TI di Kantor DPRD Kota Sorong, berdasarkan domain APO12 dari kerangka kerja COBIT 2019.

Petunjuk Pengisian: Untuk setiap pertanyaan, mohon berikan peringkat pencapaian berdasarkan kondisi saat ini di institusi Anda. Peringkat harus didasarkan pada bukti yang ada (dokumen kebijakan, SOP, notulensi rapat, laporan, hasil survei, dll.), bukan hanya asumsi.

Skala Peringkat Penilaian:

Peringkat	Nama	Persentase Pencapaian	Deskripsi
N	Not Achieved	0 - 15%	Sangat sedikit atau tidak ada bukti sama sekali bahwa aktivitas ini dilaksanakan.
P	Partially Achieved	>15% - 50%	Ada beberapa bukti bahwa aktivitas ini dilaksanakan, namun masih terdapat kelemahan yang signifikan.
L	Largely Achieved	>50% - 85%	Ada bukti yang kuat bahwa aktivitas ini dilaksanakan secara efektif, meskipun masih ada kelemahan minor.
F	Fully Achieved	>85% - 100%	Ada bukti yang lengkap dan kuat bahwa aktivitas ini dilaksanakan secara konsisten dan mencapai tujuannya.

IDENTITAS RESPONDEN	
Nama Responden	**Ningsih Maryke Fonataba, SE**
NIP/NIDN	
Unit Kerja	**Setwan Kota Sorong**
Jabatan	**Kabag. Umum**

Tanggal Pengisian	8 April 2025

Praktik 1: APO12.01 Mengumpulkan Data Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengidentifikasi dan mengumpulkan data yang relevan untuk membantu mengidentifikasi peristiwa risiko TI di masa lalu dan masa depan.	L	*Largely Achieved*	Proses berjalan, saya sering lapor jika ada masalah.
Level 2 (Managed)	2.1 Proses pengumpulan data risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	L	*Largely Achieved*	Tidak terencana, pengumpulan data hanya saat ada laporan.
	2.2 Output dari proses pengumpulan data (misalnya daftar sumber risiko) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Tidak terencana, pengumpulan data hanya saat ada laporan.
Level 3 (Established)	3.1 Proses pengumpulan data risiko telah terdefinisi dengan baik dan terstandarisasi di seluruh institusi.	P	*Partially Achieved*	Belum jadi standar, saya tidak tahu ada SOP.

Praktik 2: APO12.02 Menganalisis Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menganalisis relevansi dan signifikansi dari peristiwa risiko yang telah teridentifikasi.	F	*Fully Achieved*	Analisis risiko pasti dilakukan setelah ada laporan.
Level 2 (Managed)	2.1 Proses analisis risiko direncanakan, dipantau, dan disesuaikan untuk mencapai tujuannya.	F	*Fully Achieved*	Terlihat terkelola, hasilnya jadi dasar perbaikan layanan.
	2.2 Output dari proses analisis (misalnya laporan prioritas risiko) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Terlihat terkelola, hasilnya jadi dasar perbaikan layanan.
Level 3 (Established)	3.1 Proses analisis risiko telah terdefinisi dengan baik dan terstandarisasi menggunakan metodologi formal.	F	*Fully Achieved*	Saya percaya ada metodologi karena hasilnya konsisten.

Praktik 3: APO12.03 Memelihara Profil Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi memelihara inventaris (daftar) risiko dan atributnya (misalnya, dampak, probabilitas, pemilik).	P	*Partially Achieved*	Mungkin ada pendataan, tapi saya tidak pernah melihatnya.
Level 2 (Managed)	2.1 Proses pemeliharaan profil risiko (risk register) direncanakan, dipantau, dan disesuaikan.	N	*Not Achieved*	Belum dikelola, tidak ada *risk register* yang pernah disosialisasikan
	2.2 Output dari proses (profil risiko yang diperbarui) ditetapkan, dikendalikan, dan dipelihara secara rutin.	N	*Not Achieved*	Belum dikelola, tidak ada *risk register* yang pernah disosialisasikan
Level 3 (Established)	3.1 Proses pemeliharaan profil risiko telah terdefinisi dengan baik dan terintegrasi dengan proses lain.	N	*Not Achieved*	Belum jadi standar institusi.

Praktik 4: APO12.04 Mengartikulasikan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengkomunikasikan informasi risiko kepada para pemangku kepentingan.	P	*Partially Achieved*	Komunikasi hanya pemberitahuan lisan atau via grup chat.
Level 2 (Managed)	2.1 Proses komunikasi risiko direncanakan dan memiliki jadwal pelaporan yang jelas.	N	*Not Achieved*	Belum dikelola, tidak ada jadwal atau format laporan rutin.
	2.2 Output dari proses (misalnya laporan risiko) memiliki format yang ditetapkan dan dikendalikan.	N	*Not Achieved*	Belum dikelola, tidak ada jadwal atau format laporan rutin.
Level 3 (Established)	3.1 Proses komunikasi risiko telah terdefinisi dengan baik dan terstandarisasi.	N	*Not Achieved*	Belum ada SOP Komunikasi Risiko yang saya tahu.

Praktik 5: APO12.05 Merencanakan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi mengelola risiko dengan merencanakan tindakan respons (misalnya mitigasi, transfer, penerimaan).	F	*Fully Achieved*	Perencanaan respons pasti dilakukan.
Level 2 (Managed)	2.1 Proses perencanaan respons risiko direncanakan, dipantau, dan disesuaikan.	F	*Fully Achieved*	Terlihat terkelola, saya diinformasikan tentang rencana perbaikan.
	2.2 Output dari proses (dokumen rencana mitigasi) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Terlihat terkelola, saya diinformasikan tentang rencana perbaikan.
Level 3 (Established)	3.1 Proses perencanaan respons risiko telah terdefinisi dengan baik dan terstandarisasi.	L	*Largely Achieved*	Sudah jadi standar, dibuktikan dengan notulensi rapat yang kadang dibagikan.

Praktik 6: APO12.06 Mengimplementasikan Tanggapan Risiko

Penilaian	Pertanyaan	Peringkat (N/P/L/F)	Skala Penilaian	Bukti (Dokumen, SOP, Notulensi, dll.)
Level 1 (Performed)	1.1 Institusi menerapkan tindakan respons risiko yang telah direncanakan.	F	*Fully Achieved*	Implementasi tindakan perbaikan sudah pasti berjalan.
Level 2 (Managed)	2.1 Proses implementasi respons risiko direncanakan, dipantau, dan disesuaikan.	F	*Fully Achieved*	Terkelola baik, saya melihat langsung hasil implementasinya.
	2.2 Output dari proses (laporan implementasi) ditetapkan, dikendalikan, dan dipelihara.	L	*Largely Achieved*	Terkelola baik, saya melihat langsung hasil implementasinya.
Level 3 (Established)	3.1 Proses implementasi respons risiko telah terdefinisi dengan baik dan terstandarisasi.	L	*Largely Achieved*	Sudah jadi standar, layanan TI menjadi lebih baik.