

**EVALUASI KAPABILITAS MANAJEMEN RISIKO SPBE PEMERINTAH
KABUPATEN BLITAR MENGGUNAKAN COBIT 2019 (STUDI
KASUS : LAYANAN KINERJA PEGAWAI/E-KINERJA)**

SKRIPSI

**Oleh :
LINA MUSLIHATUS SA'ADAH
NIM. 220605110170**



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2026**

**EVALUASI KAPABILITAS MANAJEMEN RISIKO SPBE PEMERINTAH
KABUPATEN BLITAR MENGGUNAKAN COBIT 2019 (STUDI
KASUS : LAYANAN KINERJA PEGAWAI/E-KINERJA)**

SKRIPSI

Diajukan kepada:
Universitas Islam Negeri Maulana Malik Ibrahim Malang
Untuk memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Komputer (S.Kom)

Oleh :
LINA MUSLIHATUS SA'ADAH
NIM. 220605110170

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2026**

HALAMAN PERSETUJUAN

EVALUASI KAPABILITAS MANAJEMEN RISIKO SPBE PEMERINTAH KABUPATEN BLITAR MENGGUNAKAN COBIT 2019 (STUDI KASUS : LAYANAN KINERJA PEGAWAI/E-KINERJA)

SKRIPSI

Oleh :
LINA MUSLIHATUS SA'ADAH
NIM. 220605110170

Telah Diperiksa dan Disetujui untuk Diuji:
Tanggal: 14 Mei 2026

Pembimbing I,



Syahiduz Zaman, M.Kom
NIP. 19700502 200501 1 005

Pembimbing II,



Dr. M. Imamudin Lc, MA
NIP. 19740602 200901 1 010

Mengetahui,
Ketua Program Studi Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang



Supriyono, M. Kom

NIP. 198401020201903 1 012

HALAMAN PENGESAHAN

EVALUASI KAPABILITAS MANAJEMEN RISIKO SPBE PEMERINTAH KABUPATEN BLITAR MENGGUNAKAN COBIT 2019 (STUDI KASUS : LAYANAN KINERJA PEGAWAI/E-KINERJA)

SKRIPSI

Oleh :

LINA MUSLIHATUS SA'ADAH
NIM. 220605110170

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
Untuk Memperoleh Gelar Sarjana Komputer (S.Kom)
Tanggal:14 Mei 2026

Susunan Dewan Penguji

Ketua Penguji	: <u>Dr. M. Ainul Yaqin, M.Kom</u> NIP. 19761013 200604 1 004
Anggota Penguji I	: <u>Dr. Totok Chamidy, M. Kom</u> NIP. 19691222 200604 1 001
Anggota Penguji II	: <u>Syahiduz Zaman, M.Kom</u> NIP. 19700502 200501 1 005
Anggota Penguji III	: <u>Dr. M. Imamudin Lc, MA</u> NIP. 19740602 200901 1 010



Mengetahui dan Mengesahkan,
Ketua Program Studi Teknik Informatika
Fakultas Sains dan Teknologi

Universitas Islam Maulana Malik Ibrahim Malang



Suryono, M. Kom

NIP. 19841010 201903 1 012

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Lina Muslihatus Sa'adah
NIM : 220605110170
Fakultas / Program Studi : Sains dan Teknologi / Teknik Informatika
Judul Skripsi : Evaluasi Kapabilitas Manajemen Risiko SPBE
Pemerintah Kabupaten Blitar Menggunakan
COBIT 2019 (Studi Kasus : Layanan Kinerja
Pegawai / E- Kinerja)

Menyatakan dengan sebenarnya bahwa Skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambil alihan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka.

Apabila dikemudian hari terbukti atau dapat dibuktikan skripsi ini merupakan hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 20 Mei 2026
Yang membuat pernyataan,



Lina Muslihatus Sa'adah
NIM. 220605110170

MOTTO

“problems are part of the journey to success”

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur, karya ini saya persembahkan kepada:

Ayah, Ibu, dan kakak-kakak tercinta

Atas doa, dukungan, dan kasih sayang tanpa henti yang selalu menjadi
sumber kekuatan dan motivasi.

Seluruh keluarga besar

Yang senantiasa memberikan dukungan dan doa dalam setiap
langkah menyelesaikan skripsi.

Dosen pembimbing dan para pengajar

Atas bimbingan, arahan, serta ilmu yang sangat berarti bagi saya.

Teman-teman Infinity Teknik Informatika 2022

Yang telah menjadi bagian dari perjalanan ini melalui kebersamaan dan
semangat yang tidak pernah padam.

Dan akhirnya, untuk diri sendiri

Yang terus berusaha, melangkah, dan bertahan hingga mencapai titik ini.

KATA PENGANTAR

Assalamu 'alaikum Warahmatullahi Wabarakatuh

Alhamdulillahirabbil'alamin, puji syukur saya panjatkan ke hadirat Allah SWT. sehingga tugas skripsi berjudul “EVALUASI KAPABILITAS MANAJEMEN RISIKO SPBE PEMERINTAH KABUPATEN BLITAR MENGGUNAKAN COBIT 2019 (STUDI KASUS : LAYANAN KINERJA PEGAWAI/E-KINERJA)” dapat diselesaikan dengan baik. Shalawat serta salam semoga tetap tercurah kepada Nabi Muhammad SAW.

Tugas skripsi ini disusun sebagai salah satu syarat memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, UIN Maulana Malik Ibrahim Malang. Oleh karena itu, saya menyampaikan terima kasih kepada:

1. Prof. Dr. Hj. Ilfi Nur Diana, M.Si., selaku Rektor Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang.
2. Dr. H. Agus Mulyono, S.Pd., M.Kes, selaku Dekan Fakultas Sains dan Teknologi UIN Maulana Malik Ibrahim Malang.
3. Supriyono, M. Kom, selaku Ketua Program Studi Teknik Informatika UIN Maulana Malik Ibrahim Malang.
4. Syahiduz Zaman, M.Kom, selaku Dosen Pembimbing I, yang dengan kesabaran dan dedikasinya membimbing saya selama penyusunan skripsi.
5. Dr. M. Imamudin Lc, MA, selaku Dosen Pembimbing II, yang

senantiasa memberikan arahan dan masukan yang sangat berharga dalam pengerjaan skripsi ini.

6. Dr. M. Ainul Yaqin, M.Kom, dan Dr. Totok Chamidy, M.Kom, selaku Dosen Penguji yang telah memberikan kritik, saran, dan bimbingan untuk menyempurnakan skripsi ini.
7. Nia Faricha, S.Si., admin Program Studi Teknik Informatika, yang membantu dalam urusan administrasi dan selalu mengingatkan tentang kelengkapan berkas.
8. Kedua orang tua tercinta, serta kakak-kakak tercinta, yang selalu menjadi pilar kekuatan dengan doa, cinta, dan dukungan tanpa henti.
9. Seluruh keluarga, teman, dan sahabat yang turut memberikan bantuan, semangat, dukungan, dan doa untuk saya.

Saya mengucapkan terima kasih kepada diri sendiri atas usaha dan ketekunan hingga skripsi ini dapat diselesaikan. Saya menyadari bahwa penelitian dalam tugas skripsi ini masih jauh dari kata sempurna dan memiliki berbagai keterbatasan. Penelitian ini juga masih dapat dikembangkan lebih lanjut agar hasilnya semakin baik. Semoga skripsi ini bermanfaat bagi pembaca dan masyarakat.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Malang, 20 Mei 2026

Penulis

DAFTAR ISI

HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN.....	iv
PERNYATAAN KEASLIAN TULISAN	v
HALAMAN MOTTO	vi
HALAMAN PERSEMBAHAN	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xiii
ABSTRAK	xiv
ABSTRACT	xv
الملخص	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Pernyataan Masalah	5
1.3 Tujuan Penelitian	6
1.4 Manfaat Penelitian	6
1.5 Batasan Masalah.....	7
1.6 Object Penelitian (SPBE).....	9
1.7 Fokus Penelitian.....	10
BAB II KAJIAN PUSTAKA.....	12
2.1 Definisi SPBE	12
2.2 COBIT 2019.....	12
2.3 Hubungan COBIT 2019 dengan ISO 31000:2018 dan ISO/IEC 27001:2022.....	15
2.4 Manajemen Risiko dalam SPBE	30
BAB III DESAIN DAN IMPLEMENTASI	32
3.1 Desain Penelitian.....	32
3.2 Tahapan Penelitian.....	37
BAB IV HASIL DAN PEMBAHASAN	52
4.1 Deskripsi Objek dan Responden Penelitian	52
4.2 Hasil Pengolahan Data Kuisioner COBIT 2019	67
4.2.1 Domain EDM03 – Ensure Risk Optimization.....	67
4.2.2 Domain APO12 – Manage Risk.....	69
4.2.3 Domain DSS04 – Manage Continuity.....	72
4.3 Hasil Analisis Kualitatif (Wawancara 11 Responden).....	75
4.3.1 Tema Utama dari Wawancara	76
4.3.2 Temuan Per Domain.....	77
4.4 Analisis Kapabilitas Menggunakan COBIT 2019.....	81
4.4.1 Rekap Level Kapabilitas per Domain	81
4.4.2 Gap Analysis (Kondisi Existing vs Ideal)	83
4.4.3 Pembahasan	85
4.5 Integrasi Islam: Mu’amalah Allah & Mu’amalah Ma’annas	87

4.5.1 Mu'amalah kepada Allah	88
4.5.2 Mu'amalah kepada Manusia (Mu'amalah Ma'annas).....	90
BAB V PENUTUP	89
5.1 Kesimpulan	95
5.2 Saran.....	95
DAFTAR PUSTAKA	

DAFTAR GAMBAR

Gambar 2.1 Hubungan SPBE - ISO - COBIT	18
Gambar 2.2 Bagan Hubungan SPBE – ISO - COBIT.....	19
Gambar 2.3 Ilustrasi Sistem Pemerintahan Berbasis Elektronik (SPBE).....	20
Gambar 3.1 Desain Penelitian	36
Gambar 4.1 Grafik Kematangan Domain COBIT 2019 pada Layanan e-Kinerja.	82
Gambar 4.2 Skala Penentuan Level Kapabilitas COBIT 2019.....	83

DAFTAR TABEL

Tabel 2.1 Perbandingan COBIT 5 dan COBIT 2019.....	14
Tabel 2.2 Pemetaan ISO 31000 terhadap COBIT 2019	16
Tabel 2.3 Pemetaan Aspek ISO/IEC 27001 terhadap Domain COBIT 2019.	17
Tabel 2.4 Pemetaan Aspek Penilaian terhadap Standar yang Digunakan.....	18
Tabel 2.5 Pemetaan Komponen Standar terhadap Fokus dan Fungsinya dalam Penelitian.	20
Tabel 2.6 Ringkasan Penelitian Terdahulu SPBE dan COBIT 2019.....	25
Tabel 2.7 Perbandingan Standar Tata Kelola dan Manajemen Risiko Informasi.	28
Tabel 3.1 Deskripsi dan Karakteristik Data Penelitian.	33
Tabel 3.2 Ringkasan Pertanyaan dan Hasil Rata-Rata Skor Kuisisioner per Domain COBIT 2019	38
Tabel 3.3 Skala Penilaian Respondent.....	39
Tabel 3.4 Instrumen Penilaian Domain EDM03 COBIT 2019	39
Tabel 3.5 Instrumen Penilaian Domain APO12 COBIT 2019	40
Tabel 3.6 Instrumen Penilaian Domain DSS04 COBIT 2019	42
Tabel 4.1 Hasil Penilaian Kapabilitas Domain EDM03 (Ensure Risk Optimization).....	68
Tabel 4.2 Hasil Penilaian Kapabilitas Domain APO12 (Manage Risk).....	70
Tabel 4.3 Hasil Penilaian Kapabilitas Domain DSS04 (Manage Continuity)	73
Tabel 4.4 Rekapitulasi Nilai dan Level Kapabilitas Domain COBIT 2019.....	81

ABSTRAK

Lina, Lina Muslihatus Sa'adah. 2026. **Evaluasi Kapabilitas Manajemen Risiko SPBE Pemerintah Kabupaten Blitar Menggunakan COBIT 2019 (Studi Kasus : Layanan Kinerja Pegawai / E-Kinerja)**. Skripsi. Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Syahiduz Zaman, M.Kom (II) Dr. M. Imamudin Lc, MA.

Kata kunci: *Manajemen Risiko, SPBE, e-Kinerja, COBIT 2019, Kapabilitas*

Penelitian ini bertujuan untuk mengevaluasi kapabilitas manajemen risiko Sistem Pemerintahan Berbasis Elektronik (SPBE) pada layanan e-Kinerja di Dinas Komunikasi dan Informatika Kabupaten Blitar menggunakan kerangka kerja COBIT 2019 pada domain EDM03 (Ensure Risk Optimization), APO12 (Manage Risk), dan DSS04 (Manage Continuity). Metode penelitian yang digunakan adalah pendekatan campuran (mixed method) melalui kuesioner skala Likert kepada 11 responden serta wawancara dan observasi dokumen untuk memperkuat analisis. Hasil penelitian menunjukkan bahwa manajemen risiko telah dilaksanakan melalui tahapan perencanaan, identifikasi, analisis kualitatif dan kuantitatif, mitigasi, implementasi, serta monitoring, namun tingkat kapabilitasnya masih bervariasi. Domain EDM03 memperoleh nilai 2,80 (Level 3 – Established), APO12 sebesar 2,29 (Level 2 – Managed), dan DSS04 sebesar 3,40 (Level 3 – Established), yang menunjukkan bahwa proses manajemen risiko telah berjalan secara sistematis tetapi belum sepenuhnya terdokumentasi dan terstandarisasi secara formal. Dengan demikian, kapabilitas manajemen risiko SPBE pada layanan e-Kinerja berada pada tingkat Managed hingga Established, sehingga diperlukan peningkatan pada aspek dokumentasi, standarisasi prosedur, dan pemanfaatan hasil analisis risiko dalam pengambilan keputusan strategis agar mencapai tingkat kapabilitas yang lebih optimal.

ABSTRACT

Lina, Lina Muslihatus Sa'adah. 2026. **Evaluation of SPBE Risk Management Capabilities of the Blitar Regency Government Using COBIT 2019 (Case Study: Employee Performance Services / E-Performance)**. Thesis. Department of Informatics Engineering, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University, Malang. Supervisor: (I) Syahiduz Zaman, M.Kom (II) Dr. M. Imamudin Lc, MA.

Keywords: *Risk Management, SPBE, e-Performance, COBIT 2019, Capabilities*

This study aims to evaluate the risk management capabilities of the Electronic-Based Government System (SPBE) in e-Performance services at the Communication and Information Office of Blitar Regency using the COBIT 2019 framework in the domains of EDM03 (Ensure Risk Optimization), APO12 (Manage Risk), and DSS04 (Manage Continuity). The research method used was a mixed method approach through a Likert scale questionnaire to 11 respondents as well as interviews and document observations to strengthen the analysis. The results of the study show that risk management has been implemented through the stages of planning, identification, qualitative and quantitative analysis, mitigation, implementation, and monitoring, but the level of capability still varies. The EDM03 domain obtained a score of 2.80 (Level 3 – Established), APO12 of 2.29 (Level 2 – Managed), and DSS04 of 3.40 (Level 3 – Established), indicating that the risk management process has been systematically carried out but has not been fully documented and formally standardized. Thus, SPBE's risk management capabilities in e-Performance services are at the Managed to Established levels, so improvements are needed in the aspects of documentation, standardization of procedures, and the use of risk analysis results in strategic decision-making in order to achieve a more optimal level of capability.

الملخص

لينا، لينا مصلحة السعادة. ٢٠٢٦. تقييم قدرات إدارة المخاطر في SPBE لحكومة بليتار ريجنسي باستخدام COBIT ٢٠١٩ (دراسة حالة: خدمات أداء الموظفين / الأداء الإلكتروني). رسالة جامعية. قسم هندسة المعلوماتية، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية، مالانغ. المشرف: (الأول) شهيد الزمان، م. كوم (الثاني) الدكتور محمد إمام الدين ليسانس، ماجستير.

الكلمات المفتاحية: إدارة المخاطر، SPBE، الأداء الإلكتروني، COBIT ٢٠١٩، القدرات

تهدف هذه الدراسة إلى تقييم قدرات إدارة المخاطر لنظام الحكومة الإلكتروني (SPBE) في خدمات الأداء الإلكتروني في مكتب الاتصالات والمعلومات في منطقة بليتار باستخدام إطار COBIT ٢٠١٩ في مجالات EDM٠٣ (ضمان تحسين المخاطر)، APO١٢ (إدارة المخاطر)، وDSS٠٤ (إدارة الاستمرارية). كانت طريقة البحث المستخدمة منهجا مختلطاً من خلال استبيان مقياس ليكرت ل ١١ مشاركا بالإضافة إلى مقابلات وملاحظات وثائقية لتعزيز التحليل. تظهر نتائج الدراسة أن إدارة المخاطر تم تنفيذها من خلال مراحل التخطيط، والتحديد، والتحليل النوعي والكمي، والتخفيف، والتنفيذ، والمراقبة، لكن مستوى القدرة لا يزال متفاوتاً. حصل نطاق EDM٠٣ على درجة ٢.٨٠ (المستوى ٣ - المثبت)، وAPO١٢ من ٢.٢٩ (المستوى ٢ - المدار)، وDSS٠٤ من ٣.٤٠ (المستوى ٣ - المثبت)، مما يشير إلى أن عملية إدارة المخاطر قد تم تنفيذها بشكل منهجي لكنها لم يتم توثيقها بالكامل أو توحيداً رسمياً. لذا، فإن قدرات SPBE في إدارة المخاطر في خدمات الأداء الإلكتروني تقع على المستويات المدارة إلى المعتمدة، لذا هناك حاجة إلى تحسينات في جوانب التوثيق، وتوحيد الإجراءات، واستخدام نتائج تحليل المخاطر في اتخاذ القرار الاستراتيجي لتحقيق مستوى أفضل من القدرات.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada era digital telah membawa perubahan mendasar dalam tata kelola pemerintahan. Indonesia merespons tantangan tersebut melalui kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagaimana tertuang dalam Peraturan Presiden Nomor 95 Tahun 2018. SPBE dihadirkan sebagai instrumen strategis untuk meningkatkan kualitas pelayanan publik, memperkuat integrasi antar-sistem informasi, serta mendorong transparansi dan efisiensi birokrasi Tanjung et al., (2021). Idealitas yang diharapkan dari kebijakan ini adalah terciptanya tata kelola pemerintahan yang modern, efektif, dan terpercaya, sehingga mampu memberikan pelayanan publik yang lebih cepat, akurat, dan responsif.

Namun demikian, di balik potensi besar tersebut terdapat problematika nyata yang tidak dapat diabaikan. Ketergantungan terhadap teknologi informasi menjadikan sistem pemerintahan rentan terhadap ancaman seperti kebocoran data, serangan siber, gangguan sistem, hingga kegagalan layanan public Anugrah et al., (2022). Berbagai penelitian menunjukkan bahwa kapabilitas manajemen risiko informasi di instansi pemerintah daerah masih tergolong rendah, buktinya sepanjang tahun 2023 terdapat 103 insiden dugaan kebocoran data di Indonesia, dengan mayoritas (sekitar 69 %) terjadi di sektor administrasi pemerintahan.

Lebih lanjut, data menunjukkan bahwa selama rentang empat tahun

terakhir telah tercatat 94,22 juta data penduduk Indonesia yang dilaporkan bocor.

Kondisi seperti ini menunjukkan bahwa kapabilitas manajemen risiko informasi di instansi pemerintah masih sangat rentan, sehingga perlu ditindaklanjuti secara sistematis. (Sumber: *Databoks Katadata, “Kebocoran Data RI Terbanyak dari Sektor Pemerintahan”, 2023; CNN Indonesia, “RI Masuk 10 Besar Negara dengan Kebocoran Data Tertinggi, Hampir 100 Juta Data”, 2024*). Khususnya pada domain EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*) dan DSS04 (*Manage Continuity*) dalam kerangka kerja COBIT 2019 Taryoko et al., (2024). Kondisi ini menggambarkan adanya gap antara idealitas tata kelola yang diharapkan dengan realitas implementasi di lapangan, di mana proses identifikasi, mitigasi, serta evaluasi risiko belum terdokumentasi dan terintegrasi secara optimal. Al-Qur'an sebagai petunjuk hidup umat Islam sejatinya telah memberikan isyarat tentang pentingnya kehati-hatian dan manajemen risiko dalam setiap

aktivitas manusia. Allah SWT berfirman dalam QS. Al-Hasyr ayat 18:

يَا أَيُّهَا الَّذِينَ آمَنُوا اتَّقُوا اللَّهَ وَلْتَنْظُرْ نَفْسٌ مَّا قَدَّمَتْ لِإِعَادٍ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ خَبِيرٌ بِمَا تَعْمَلُونَ ﴿١٨﴾

“Wahai orang-orang yang beriman, bertakwalah kepada Allah dan hendaklah setiap diri memperhatikan apa yang telah diperbuatnya untuk hari esok. Dan bertakwalah kepada Allah; sesungguhnya Allah Maha Mengetahui apa yang kamu kerjakan.” (QS. Al-Hasyr:18)

Menurut *Tafsir Ibn Katsir*, ayat ini mengandung perintah agar setiap mukmin memperhatikan amal yang telah dilakukan untuk bekal di akhirat, dengan sikap hati-hati, penuh perhitungan menegaskan pentingnya melakukan evaluasi dan pengelolaan risiko atas setiap langkah kehidupan (Nasution et al., 2024).

Dalam *Tafsir Al-Muyassar* dijelaskan bahwa Allah SWT memerintahkan orang-orang beriman untuk selalu bertakwa dan melihat konsekuensi dari setiap amal yang dikerjakan, baik yang berdampak duniawi maupun ukhrawi (Sule & Mainiyo, 2024). Prinsip ini relevan dengan konsep manajemen risiko, di mana setiap keputusan harus mempertimbangkan potensi ancaman dan dampaknya.

Korelasi dengan tema penelitian adalah bahwa pengelolaan risiko informasi dalam SPBE dapat dipahami sebagai implementasi nilai Qur'ani dalam konteks modern. Sebagaimana ayat ini mengajarkan kewajiban antisipasi terhadap “hari esok”, maka instansi pemerintah juga dituntut untuk melakukan mitigasi risiko agar layanan publik tetap berkelanjutan, aman, dan terpercaya. Islam sejak awal telah menanamkan budaya antisipasi dan perencanaan. Prinsip tersebut selaras dengan pengelolaan risiko informasi SPBE sebagai wujud implementasi nilai Qur'ani dalam tata kelola modern.

Ayat ini mengajarkan prinsip antisipasi, perencanaan, dan evaluasi risiko sebelum mengambil keputusan, yang selaras dengan konsep manajemen risiko modern. Dengan demikian, penelitian dalam bidang Teknologi Informasi tidak hanya berdiri pada landasan teoritis sains, melainkan juga dikawal oleh nilai-nilai Islam yang mendorong umatnya untuk berpikir kritis (pikir) sekaligus berdzikir dalam mengelola potensi dan ancaman yang dihadapi.

Guna menjawab permasalahan masih rendahnya kapabilitas manajemen risiko informasi di instansi pemerintah yang ditunjukkan oleh maraknya insiden kebocoran data, lemahnya dokumentasi proses manajemen risiko, serta belum

optimalnya integrasi tata kelola risiko dengan kebijakan SPBE, penelitian ini berfokus pada evaluasi kapabilitas manajemen risiko informasi SPBE di Pemerintah Kabupaten Blitar menggunakan kerangka kerja COBIT 2019. Framework ini dipilih karena memiliki pendekatan yang fleksibel, adaptif, dan terintegrasi dengan standar internasional seperti ISO 31000:2018 dan ISO/IEC 27001. Evaluasi dilakukan tidak hanya untuk mengukur kondisi eksisting, tetapi juga untuk mengidentifikasi kesenjangan terhadap kondisi ideal yang seharusnya dicapai Yohana, (2022). Dengan hasil tersebut, diharapkan dapat disusun rekomendasi perbaikan yang komprehensif, terukur, dan sesuai dengan kebijakan nasional.

Urgensi penelitian ini semakin nyata ketika dikaitkan dengan visi besar pemerintah dalam mewujudkan pemerintahan digital yang efektif, aman, dan berkelanjutan Kunio et al., (2022). Dengan memperkuat kapabilitas manajemen risiko informasi, instansi pemerintah tidak hanya mampu menjaga keberlangsungan layanan publik, tetapi juga memperkuat kepercayaan masyarakat terhadap pemerintahan Taufik et al., (2023). Hal ini sejalan dengan misi Islam yang mengajarkan amanah, profesionalitas, dan tanggung jawab dalam mengelola segala aspek kehidupan, termasuk dalam tata kelola teknologi informasi. Oleh karena itu, penelitian ini layak untuk dilakukan sebagai kontribusi ilmiah sekaligus pengabdian nyata dalam mewujudkan pemerintahan yang transparan.

Selain itu, penelitian ini menjadi penting karena hingga saat ini manajemen risiko SPBE di Dinas Komunikasi dan Informatika Kabupaten Blitar belum pernah dievaluasi secara menyeluruh. Padahal, sistem informasi yang

dikelola oleh instansi tersebut memiliki peran krusial dalam mendukung pelayanan publik dan menjadi tulang punggung keterbukaan data pemerintah daerah. Risiko seperti kebocoran data, gangguan sistem, serta keluhan masyarakat terhadap layanan digital menunjukkan bahwa pengelolaan risiko informasi masih perlu diperkuat. Oleh karena itu, penelitian ini berupaya memberikan evaluasi mendalam untuk meningkatkan kapabilitas manajemen risiko SPBE di lingkungan Pemerintah Kabupaten Blitar.

1.2 Pernyataan Masalah

Berdasarkan latar belakang tersebut, dapat diidentifikasi bahwa implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) di instansi pemerintah masih menghadapi sejumlah tantangan, terutama dalam hal manajemen risiko informasi.

Berbagai penelitian dan laporan menunjukkan masih rendahnya kapabilitas tata kelola risiko, yang ditandai dengan lemahnya dokumentasi proses, belum adanya evaluasi berkelanjutan, serta masih sering terjadinya kebocoran data di lingkungan pemerintahan. Kondisi ini menimbulkan pertanyaan mendasar:

Bagaimana cara memastikan bahwa pengelolaan risiko informasi pada sistem SPBE (khususnya sistem e-Kinerja) berjalan secara efektif, terdokumentasi, dan selaras dengan tujuan organisasi serta standar nasional dan internasional. Maka fokus masalah yang akan diselesaikan, yaitu :

1. menilai kapabilitas manajemen risiko informasi SPBE (khususnya e-Kinerja) menggunakan COBIT 2019
2. memberikan rekomendasi perbaikan.

1.3 Tujuan Penelitian

Untuk mengevaluasi kapabilitas manajemen risiko informasi SPBE pada Pemerintah Kabupaten Blitar menggunakan kerangka kerja COBIT 2019.

1.4 Manfaat Penelitian

Penelitian ini diharapkan tidak hanya menjawab permasalahan yang dirumuskan, tetapi juga memberi kontribusi bagi pengembangan ilmu dan praktik tata kelola SPBE. Manfaat penelitian ini adalah sebagai berikut:

- a. Penelitian ini dapat memperkaya literatur akademik di bidang tata kelola teknologi informasi, khususnya mengenai penerapan kerangka kerja COBIT 2019 pada manajemen risiko SPBE. Hasil penelitian ini juga dapat menjadi referensi bagi penelitian selanjutnya dalam bidang serupa maupun bidang kajian teknologi informasi yang terkait dengan manajemen risiko dan keamanan data.
- b. Bagi Pemerintah Kabupaten Blitar, penelitian ini bermanfaat sebagai bahan evaluasi untuk mengetahui tingkat kapabilitas manajemen risiko informasi pada SPBE. Selain itu, hasil penelitian ini dapat digunakan sebagai dasar penyusunan strategi peningkatan tata kelola risiko yang lebih sistematis, Kabupaten Blitar berdasarkan sehingga layanan publik berbasis digital menjadi lebih andal, aman, dan berkesinambungan.
- c. Penelitian ini dapat memberikan rekomendasi yang relevan dan terukur guna mendukung penerapan kebijakan nasional terkait SPBE dan manajemen risiko informasi. Dengan demikian, penelitian ini layak dilakukan karena selaras dengan kebutuhan pembangunan pemerintahan digital yang efektif,

transparan, dan berkelanjutan.

1.5 Batasan Masalah

Agar penelitian lebih terarah, maka ruang lingkup penelitian ini dibatasi pada hal-hal berikut:

1. **Objek Penelitian** : Penelitian hanya dilakukan pada Pemerintah Kabupaten Blitar, khususnya unit kerja yang terkait dengan pengelolaan dan penerapan SPBE. Penelitian tidak mencakup instansi pemerintah daerah lain atau lembaga swasta.
 - a. Penelitian ini menggunakan kerangka kerja COBIT 2019 sebagai alat evaluasi kapabilitas manajemen risiko. COBIT 2019 dipilih karena merupakan versi terbaru yang telah menyempurnakan COBIT 5 dengan pendekatan yang lebih komprehensif terhadap tata kelola teknologi informasi, termasuk integrasi dengan standar internasional seperti ISO 31000:2018 dan ISO/IEC 27001:2022.
 - b. Objek penelitian difokuskan pada satu sistem SPBE, yaitu Layanan Kinerja Pegawai (*e-Kinerja*) di Pemerintah Kabupaten Blitar yang dikelola oleh Dinas Komunikasi dan Informatika Kabupaten Blitar. Sistem ini dipilih karena bersifat krusial dalam pelayanan publik dan memiliki tingkat risiko informasi yang tinggi sehingga relevan untuk dianalisis menggunakan COBIT 2019.
2. **Domain COBIT 2019** : Evaluasi kapabilitas manajemen risiko difokuskan pada domain EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*) dan DSS04 (*Manage Continuity*). Domain lain seperti BAI10 (*Manage*

Configuration) tidak menjadi fokus utama dalam penelitian ini.

3. **Metode dan Data Penelitian** : Data penelitian diperoleh kerangka kerja COBIT melalui studi literatur, kuesioner, wawancara, dan observasi di lapangan. Penelitian tidak membahas aspek teknis detail seperti konfigurasi perangkat lunak atau implementasi sistem keamanan jaringan.
4. **Standar Acuan** : Penelitian ini hanya menggunakan standar COBIT 2019, ISO 31000:2018, ISO/IEC 27001:2022, serta Permenpan-RB No. 5 Tahun 2020 sebagai kerangka evaluasi. Standar lain yang tidak disebutkan tidak dijadikan rujukan dalam penelitian.

Dengan adanya batasan masalah tersebut, penelitian ini diharapkan dapat lebih fokus dan terarah pada aspek yang paling relevan dengan tujuan penelitian. Batasan ini juga membantu peneliti menghindari pembahasan yang terlalu luas, sehingga analisis yang dilakukan tetap mendalam dan sesuai dengan kapasitas penelitian. Selain itu, ruang lingkup yang jelas akan memudahkan dalam penyusunan instrumen penelitian, proses pengumpulan data, serta penyusunan rekomendasi yang lebih tepat sasaran bagi Pemerintah Kabupaten Blitar.

Penetapan batasan juga penting untuk menjaga konsistensi penelitian. Karena objek penelitian hanya difokuskan pada Pemerintah Kabupaten Blitar, maka hasil evaluasi dan rekomendasi yang dihasilkan akan benar-benar kontekstual dengan kondisi yang ada di instansi tersebut Rahmawati, (2023). Fokus pada dua domain COBIT 2019, yaitu EDM03, APO12 dan DSS04, membuat penelitian lebih tajam dalam menganalisis aspek manajemen risiko, tanpa harus melebar ke domain lain yang mungkin memerlukan penelitian terpisah Aryati et al., (2023). Begitu juga dengan penggunaan standar COBIT

2019, ISO 31000:2018, dan ISO/IEC 27001:2022 sebagai acuan utama, hal ini akan memperkuat validitas teori sekaligus menjaga agar kerangka evaluasi tetap konsisten.

Dengan demikian, batasan masalah yang ditetapkan bukanlah sebuah pengurangan nilai penelitian, melainkan justru strategi agar penelitian ini lebih terarah, mendalam, dan menghasilkan rekomendasi yang praktis serta aplikatif. Hasil yang diperoleh nantinya diharapkan tidak hanya bermanfaat secara akademis, tetapi juga dapat menjadi masukan nyata bagi Pemerintah Kabupaten Blitar dalam meningkatkan kapabilitas pengelolaan risiko informasi di lingkungan SPBE.

Layanan Kinerja Pegawai (*e-Kinerja*) dipilih karena berperan langsung dalam pengelolaan kinerja aparatur, menjadi dasar evaluasi prestasi kerja, serta terintegrasi dengan layanan SPBE lainnya. Sistem ini krusial karena berhubungan dengan data pribadi ASN, evaluasi kinerja, dan transparansi birokrasi, sehingga memiliki tingkat risiko tinggi apabila terjadi gangguan atau kebocoran informasi.

1.6 Objek Penelitian (SPBE)

Sistem Pemerintahan Berbasis Elektronik (SPBE) di Pemerintah Kabupaten Blitar diteliti tentang sistem digital untuk mengelola dan menilai kinerja Aparatur Sipil Negara (ASN). Selain itu mencakup berbagai layanan digital seperti:

- a. **e-Kinerja** (Layanan Kinerja Pegawai)
- b. **e-Office** (Surat-menyurat digital dan disposisi elektronik)
- c. **e-Planning** (Perencanaan pembangunan daerah)
- d. **e-Budgeting** (Perencanaan dan pelaporan anggaran)

- e. **e-SAKIP** (Sistem Akuntabilitas Kinerja Instansi Pemerintah)
- f. serta sistem lain yang mendukung integrasi data pemerintahan.

Dari berbagai sistem tersebut, penelitian ini memilih Layanan Kinerja Pegawai (*e- Kinerja*) sebagai objek utama karena:

1. Sistem ini **krusial** dalam mendukung penilaian kinerja aparatur sipil negara (ASN).
2. **Terintegrasi langsung** dengan sistem SPBE lain seperti e-SAKIP dan e-Office.
3. **Berisiko tinggi** terhadap kebocoran data pribadi ASN serta gangguan sistem yang dapat mempengaruhi pelayanan publik.

Penelitian ini difokuskan pada sistem *e-Kinerja* karena sistem ini paling krusial dalam pengelolaan kinerja ASN, memiliki potensi risiko kebocoran data pegawai yang tinggi, serta terintegrasi dengan sistem SPBE lainnya. Oleh karena itu, *e-Kinerja* dinilai paling relevan untuk dianalisis menggunakan kerangka kerja COBIT 2019, khususnya dalam domain EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan DSS04 (*Manage Continuity*).

1.7 Fokus Penelitian

Penelitian ini tidak mencakup seluruh sistem SPBE yang ada di Pemerintah Kabupaten Blitar, melainkan difokuskan pada satu sistem, yaitu Layanan Kinerja Pegawai (*e-Kinerja*), agar analisis kapabilitas manajemen risiko dapat dilakukan secara mendalam dan terukur.

E-Kinerja dipilih karena merupakan sistem digital yang krusial, digunakan untuk mengelola data kinerja aparatur sipil negara (ASN), penilaian prestasi kerja,

dan integrasi laporan kinerja instansi.

Fokus penelitian ini adalah mengevaluasi kapabilitas manajemen risiko informasi pada sistem e-Kinerja menggunakan kerangka kerja COBIT 2019, dengan domain EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan DSS04 (*Manage Continuity*).

Dengan pembatasan fokus ini, penelitian dapat dilakukan secara lebih mendalam dan menghasilkan rekomendasi yang spesifik serta aplikatif untuk meningkatkan tata kelola risiko informasi SPBE di lingkungan Pemerintah Kabupaten Blitar.

BAB II

KAJIAN PUSTAKA

2.1 Definisi SPBE

Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada instansi pemerintah, aparatur, pelaku usaha, dan masyarakat secara terintegrasi Borysenko, (2023). SPBE mencakup seluruh proses tata kelola pemerintahan yang berjalan secara digital, mulai dari administrasi, pengelolaan data, hingga layanan publik berbasis elektronik.

Secara konsep, SPBE dapat dianalogikan seperti ERP (*Enterprise Resource Planning*) pada sektor pemerintahan, di mana seluruh sistem saling terhubung dan berbagi data secara terpadu Chen, (2023). Dengan integrasi ini, setiap unit kerja dalam pemerintahan dapat saling bertukar informasi, mempercepat proses pelayanan, serta meningkatkan efisiensi dan transparansi penyelenggaraan pemerintahan.

SPBE tidak hanya berfungsi sebagai sistem teknis, tetapi juga sebagai strategi nasional dalam mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel. Dalam konteks ini, penerapan SPBE memerlukan pengelolaan risiko informasi yang baik agar seluruh sistem yang digunakan dapat berjalan aman, handal, dan berkesinambungan.

2.2 COBIT 2019

COBIT (*Control Objectives for Information and Related Technologies*)

adalah kerangka kerja internasional yang digunakan untuk membantu organisasi dalam mengelola, mengontrol, dan memastikan tata kelola Teknologi Informasi (TI) berjalan efektif. Framework ini pertama kali dikembangkan oleh ISACA (*Information Systems Audit and Control Association*) pada tahun 1996, dan terus diperbarui untuk menyesuaikan dengan perkembangan teknologi serta kebutuhan organisasi modern.

Perkembangan Versi COBIT

1. **COBIT 1 (1996)** – Dikenalkan pertama kali sebagai pedoman audit untuk sistem informasi. Fokus utamanya adalah memastikan kontrol TI agar sejalan dengan kebutuhan bisnis.
2. **COBIT 2 (1998)** – Menambahkan panduan manajemen TI dan memperluas cakupan dari sekadar audit menjadi alat bantu pengelolaan TI.
3. **COBIT 3 (2000)** – Memperkenalkan konsep *maturity level* dan *performance measurement*, yang membantu organisasi menilai tingkat kematangan tata kelola TI.
4. **COBIT 4 dan 4.1 (2005–2007)** – Menyempurnakan integrasi dengan standar lain seperti ITIL dan ISO 27001, serta menambahkan panduan tentang pengukuran kinerja.
5. **COBIT 5 (2012)** – Merupakan lompatan besar dengan memperluas cakupan ke seluruh tata kelola perusahaan (*enterprise governance of IT*). COBIT 5 menggabungkan prinsip, proses, dan panduan implementasi yang komprehensif untuk mencapai tujuan bisnis.
6. **COBIT 2019 (dirilis akhir 2018)** – Versi terbaru yang merupakan

penyempurnaan dari COBIT 5. COBIT 2019 memperkenalkan konsep tata kelola yang lebih fleksibel, mendukung integrasi dengan standar lain seperti ISO 31000, ISO/IEC 27001, dan ITIL 4, serta memperbarui struktur domain menjadi lebih mudah diterapkan di era digital.

Tabel 2.1 Perbandingan COBIT 5 dan COBIT 2019

Aspek	COBIT 5	COBIT 2019
Rilis	Tahun 2012	Akhir 2018
Struktur Domain	5 domain utama (EDM, APO, BAI, DSS, MEA)	Tetap 5 domain, namun indikator dan praktik diperbarui agar lebih kontekstual
Framework Pendukung	Terpisah dari standar lain	Terintegrasi dengan ISO 31000, ISO/IEC 27001, dan ITIL 4
Level Kapabilitas	Menggunakan <i>Process Maturity Model</i>	Menggunakan <i>Capability Level 0–5</i> yang lebih rinci
Konteks Digital	Belum menyesuaikan dengan era transformasi digital	Sudah menyesuaikan dengan kebutuhan transformasi digital dan risiko siber
Kelebihan	Komprehensif namun masih kaku	Lebih fleksibel dan relevan dengan kondisi organisasi saat ini

COBIT 2019 digunakan sebagai kerangka evaluasi utama dengan fokus pada tiga domain, yaitu EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan DSS04 (*Manage Continuity*), yang relevan untuk menilai kapabilitas manajemen risiko informasi dalam konteks SPBE.

Alasan Pemilihan COBIT 2019 Penelitian ini menggunakan COBIT 2019 karena merupakan versi terbaru yang lebih relevan dengan tata kelola dan manajemen risiko pada era digital. COBIT 2019 tidak hanya fokus pada kepatuhan dan audit, tetapi juga pada bagaimana risiko informasi dapat dikendalikan dan dioptimalkan agar mendukung tujuan organisasi.

Selain itu, COBIT 2019 memiliki keunggulan karena:

- a. Dapat diintegrasikan dengan ISO 31000:2018 (untuk manajemen risiko) dan ISO/IEC 27001:2022 (untuk keamanan informasi).
- b. Menyediakan tingkatan kapabilitas (0–5) yang memudahkan dalam menilai tingkat kematangan proses TI.
- c. Memberikan panduan jelas dalam mengelola domain seperti EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan DSS04 (*Manage Continuity*) yang relevan dengan penelitian ini.

COBIT 2019 menjadi pilihan paling tepat untuk mengevaluasi kapabilitas manajemen risiko informasi SPBE di Dinas Komunikasi dan Informatika Kabupaten Blitar, karena framework ini mampu memberikan hasil yang terukur, sistematis, dan dapat dijadikan dasar untuk rekomendasi perbaikan berkelanjutan.

2.3 Hubungan COBIT 2019 dengan ISO 31000:2018 dan ISO/IEC 27001:2022

Dalam penerapan tata kelola Teknologi Informasi di instansi pemerintah, penggunaan satu kerangka kerja saja sering kali tidak cukup untuk menggambarkan keseluruhan aspek pengelolaan risiko dan keamanan informasi Mr. N. Suresh et al., (2024). Oleh karena itu, penelitian ini menggabungkan prinsip dari COBIT 2019 dengan dua standar internasional lain, yaitu ISO 31000:2018 dan ISO/IEC 27001:2022, agar hasil evaluasi menjadi lebih komprehensif dan dapat dipertanggungjawabkan.

1. Hubungan COBIT 2019 dengan ISO 31000:2018 (Manajemen Risiko)

ISO 31000:2018 adalah standar internasional yang berfokus pada kerangka

kerja dan prinsip manajemen risiko. Standar ini membantu organisasi dalam mengidentifikasi, menilai, dan mengendalikan risiko yang dapat memengaruhi pencapaian tujuan organisasi.

Sementara itu, COBIT 2019 juga memuat prinsip pengelolaan risiko, khususnya dalam domain EDM03 (*Ensure Risk Optimization*) , APO12 (*Manage Risk*) dan DSS04 (*Manage Continuity*). Ketiga domain tersebut memiliki kesesuaian langsung dengan tahapan ISO 31000, seperti:

Tabel 2.2 Pemetaan ISO 31000 terhadap COBIT 2019

Tahapan ISO 31000	Domain COBIT 2019 yang Relevan	Penjelasan Singkat
Identifikasi Risiko	APO12.02 – <i>Identify Risk</i>	Organisasi mengidentifikasi potensi risiko terhadap layanan TI dan SPBE
Analisis Risiko	APO12.03 – <i>Analyze Risk</i>	Risiko yang teridentifikasi dianalisis berdasarkan dampak dan kemungkinan
Evaluasi Risiko	EDM03.02 – <i>Evaluate Risk</i>	Hasil analisis digunakan untuk mengevaluasi sejauh mana risiko dapat diterima
Penanganan Risiko	APO12.04 – <i>Manage Risk</i>	Organisasi menentukan tindakan pengendalian atau mitigasi yang diperlukan
Pemantauan & Review	EDM03.03 – <i>Monitor Risk</i>	Risiko dipantau secara berkala untuk memastikan efektivitas tindakan pengendalian
Keberlanjutan Layanan	DSS04 – <i>Manage Continuity</i>	Menjamin kelangsungan layanan dan pemulihan sistem pasca insiden atau gangguan.

Melalui integrasi ini, COBIT 2019 berfungsi sebagai alat ukur kapabilitas tata kelola, sedangkan ISO 31000 berfungsi sebagai pedoman proses manajemen risiko. Kombinasi keduanya memastikan evaluasi tidak hanya menilai kematangan proses, tetapi juga efektivitas dalam mengendalikan risiko.

2. Hubungan COBIT 2019 dengan ISO/IEC 27001:2022 (Keamanan

Informasi) ISO/IEC 27001:2022 merupakan standar internasional yang mengatur penerapan Sistem Manajemen Keamanan Informasi (SMKI).

Standar ini menekankan pentingnya menjaga kerahasiaan, integritas, dan ketersediaan informasi (*Confidentiality, Integrity, Availability –CIA*). COBIT 2019 dan ISO/IEC 27001 memiliki keterkaitan erat dalam hal kontrol dan keamanan informasi, terutama dalam domain:

Tabel 2.3 Pemetaan Aspek ISO/IEC 27001 terhadap Domain COBIT 2019

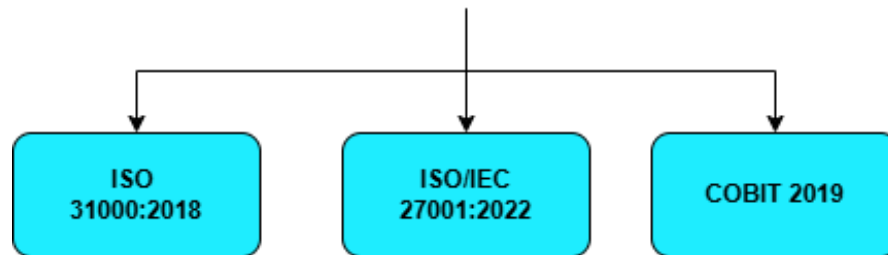
Aspek ISO/IEC 27001	Domain COBIT 2019 yang Relevan	Penjelasan
Evaluasi Risiko Keamanan	APO12 – Manage Risk	Menilai dan mengendalikan risiko keamanan informasi yang berpotensi mengganggu layanan SPBE.
Optimalisasi Risiko	EDM03 – Ensure Risk Optimization	Memastikan risiko keamanan dan operasional berada pada tingkat yang dapat diterima manajemen.
Keberlangsungan Layanan & Pemulihan Sistem	DSS04 – Manage Continuity	Menjamin kelangsungan layanan dan pemulihan data/sistem pasca gangguan atau insiden keamanan.

Maka , ISO/IEC 27001:2022 memperkuat aspek keamanan teknis dan pengendalian akses, sementara COBIT 2019 memastikan keamanan tersebut dikelola dalam kerangka tata kelola TI yang strategis dan terukur.

3. Keterpaduan Ketiga Standar

Posisi masing-masing standar dalam konteks SPBE, berikut disajikan Tabel Hubungan SPBE – ISO – COBIT, yang menunjukkan keterkaitan antara aspek yang dinilai, standar yang digunakan, dan tujuan pengukurannya.

PENGUKURAN KINERJA SPBE



Gambar 2.1 Hubungan SPBE – ISO – COBIT

Gambar ini menunjukkan bahwa pengukuran kinerja SPBE dapat dilakukan melalui tiga standar utama, yaitu ISO 31000:2018 untuk manajemen risiko, ISO/IEC 27001:2022 untuk keamanan informasi, dan COBIT 2019 untuk tata kelola serta kapabilitas TI.

Tabel 2.4 Pemetaan Aspek Penilaian terhadap Standar yang Digunakan

Aspek yang Dinilai	Standar yang Digunakan	Tujuan
Manajemen Risiko	ISO 31000:2018	Standar umum manajemen risiko
Keamanan Informasi	ISO/IEC 27001:2022	Standar keamanan informasi
Tata Kelola & Kapabilitas TI	COBIT 2019	Evaluasi kematangan dan efektivitas proses TI

Berdasarkan hasil pemetaan tersebut, dapat disimpulkan bahwa ISO berfungsi sebagai standar eksternal yang menjadi acuan internasional dalam penerapan manajemen risiko dan keamanan informasi, sedangkan COBIT berperan sebagai alat ukur internal yang menilai sejauh mana tata kelola dan proses organisasi telah berjalan secara efektif.

Maka, kombinasi antara ISO dan COBIT memungkinkan evaluasi dilakukan secara menyeluruh — baik dari aspek kepatuhan terhadap standar

global maupun kapabilitas internal organisasi dalam mengelola risiko dan tata kelola teknologi informasi.



Gambar 2.2 Bagan Hubungan SPBE – ISO – COBIT

Keterangan:

- a. **SPBE** adalah payung utama sistem digital pemerintahan.
- b. **ISO 31000:2018** memastikan pengelolaan risiko dilakukan secara sistematis.
- c. **ISO/IEC 27001:2022** menjamin keamanan dan kerahasiaan data.
- d. **COBIT 2019** menilai sejauh mana tata kelola dan manajemen risiko TI telah berjalan efektif berdasarkan kapabilitas proses.



Gambar 2.3 Ilustrasi Sistem Pemerintahan Berbasis Elektronik (SPBE)

Gambar ini menggambarkan SPBE sebagai platform terintegrasi yang menghubungkan berbagai layanan digital pemerintah, seperti e-kepegawaian, e-dokumen, e-pajak, e-keuangan, e-perizinan, dan sistem lainnya. Seluruh subsistem ini saling berinteraksi untuk meningkatkan efisiensi, transparansi, serta tata kelola pemerintahan berbasis teknologi informasi.

Ketiga standar — COBIT 2019, ISO 31000:2018, dan ISO/IEC 27001:2022 saling melengkapi satu sama lain.

Hubungan antara ketiganya dapat digambarkan sebagai berikut:

Tabel 2.5 Pemetaan Komponen Standar terhadap Fokus dan Fungsinya dalam Penelitian

Komponen	Fokus Utama	Fungsi dalam Penelitian
COBIT 2019	Tata kelola dan kapabilitas proses TI	Menilai sejauh mana penerapan manajemen risiko berjalan efektif
ISO 31000:2018	Proses manajemen risiko	Memberikan panduan sistematis dalam mengidentifikasi dan mengendalikan risiko
ISO/IEC 27001:2022	Keamanan informasi	Memastikan perlindungan data dan pencegahan kebocoran informasi

Menggabungkan ketiganya, penelitian ini dapat memberikan evaluasi yang lebih utuh dan komprehensif terhadap pengelolaan risiko informasi SPBE, baik dari sisi tata kelola, proses, maupun keamanan data.

SPBE hadir untuk menjawab kebutuhan akan tata kelola pemerintahan yang lebih efektif, efisien, transparan, dan akuntabel di era digital. SPBE memiliki peran strategis dalam mewujudkan tata kelola pemerintahan yang efektif, namun masih menghadapi tantangan dalam aspek pengelolaan risiko dan keamanan informasi Cerqueira Junior & Arima, (2023). Tantangan ini mencakup ancaman kebocoran data, gangguan sistem, hingga serangan siber yang dapat menghambat penyelenggaraan layanan publik. Namun, pelaksanaan SPBE bukan tanpa tantangan Lubna et al., (2023). Ketergantungan terhadap teknologi informasi membawa risiko yang serius, seperti kebocoran data, gangguan sistem, serangan siber, hingga kegagalan layanan publik Nafi'ah, (2022). Risiko-risiko ini, apabila tidak dikelola dengan baik, dapat berakibat pada terganggunya keberlangsungan layanan, rusaknya reputasi instansi, dan menurunnya tingkat kepercayaan masyarakat terhadap pemerintah Lompoliu & William Tangka, (2024). Oleh sebab itu, keberhasilan implementasi SPBE tidak hanya ditentukan oleh kecanggihan teknologi yang digunakan, melainkan juga sejauh mana tata kelola risiko informasi dijalankan secara sistematis dan berkesinambungan.

Dalam konteks tata kelola SPBE, manajemen risiko informasi memegang peranan yang sangat penting. Manajemen risiko dipahami sebagai suatu proses sistematis yang melibatkan kegiatan identifikasi, analisis, evaluasi, penanganan, hingga pemantauan risiko Purnomo, (2023). Tujuan dari manajemen risiko adalah

memastikan bahwa setiap ancaman yang berpotensi menimbulkan gangguan dapat dikendalikan sedini mungkin sehingga tidak mengganggu tujuan organisasi Ningtyas et al., (2023). Pemerintah Indonesia telah mengatur manajemen risiko SPBE melalui Permenpan-RB Nomor 5 Tahun 2020. Regulasi ini mengamanatkan agar setiap instansi pemerintah menjalankan siklus pengelolaan risiko yang meliputi tahap identifikasi risiko, analisis risiko, evaluasi risiko, serta perencanaan mitigasi Boniface Okanga, (2023). Selain itu, dalam praktiknya manajemen risiko SPBE juga dapat diperkuat dengan menggunakan standar internasional. ISO 31000:2018 misalnya, memberikan kerangka kerja manajemen risiko yang bersifat umum dan dapat diterapkan lintas sektor, sedangkan ISO/IEC 27001:2022 berfokus pada sistem manajemen keamanan informasi, yang mengatur bagaimana suatu organisasi melindungi kerahasiaan, integritas, dan ketersediaan informasi Yanuhar et al., (2022). Kombinasi pedoman nasional dan standar internasional tersebut menjadi landasan penting agar pengelolaan risiko SPBE berjalan lebih komprehensif dan sesuai praktik terbaik global.

Selain aturan dan standar internasional, terdapat pula kerangka kerja yang sudah diakui secara luas dalam bidang tata kelola teknologi informasi, yaitu COBIT (*Control Objectives for Information and Related Technologies*). COBIT 2019 sebagai versi terbaru menawarkan pendekatan yang lebih fleksibel, adaptif, dan integratif Lompoliu & William Tangka, (2024). Kerangka ini menekankan bahwa tata kelola TI harus selaras dengan tujuan organisasi serta mampu memastikan pengelolaan risiko yang optimal.

COBIT 2019 memiliki berbagai domain, namun dalam penelitian ini

difokuskan pada EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*) dan DSS04 (*Manage Continuity*). Domain EDM03 membahas tentang bagaimana organisasi memastikan risiko dikelola pada tingkat optimal sesuai dengan tujuan bisnis, dan APO12 menekankan pengelolaan risiko operasional secara sistematis mulai dari identifikasi, analisis, mitigasi, hingga monitoring, sementara DSS04 berfokus pada keberlanjutan layanan (*business continuity*) untuk menjamin ketersediaan sistem, pemulihan data, serta kelangsungan operasional SPBE ketika terjadi insiden atau gangguan Nisa' et al., (2023). Dengan model kapabilitas yang dimulai dari Level 0 (*Incomplete*) hingga Level 5 (*Optimizing*), COBIT 2019 memungkinkan organisasi mengukur sejauh mana praktik tata kelola risiko telah berjalan, apakah hanya bersifat dasar atau sudah mencapai tingkat berkelanjutan dan strategis.

Sejumlah penelitian terdahulu menunjukkan bahwa kapabilitas manajemen risiko informasi di Indonesia masih relatif rendah. Sari dan Juwairiah (2023) misalnya, dalam penelitian yang dilakukan pada DISKOMINFO Kabupaten Blitar, menemukan bahwa tingkat kapabilitas pada domain EDM03, APO12 dan DSS04 baru berada di Level 2 (*Managed*). Kondisi ini menunjukkan bahwa meskipun sudah ada proses manajemen risiko, namun dokumentasi dan evaluasi belum dilakukan secara konsisten. Penelitian Enrique dan Fianty (2023) pada perusahaan jasa TI di Indonesia mengungkapkan bahwa banyak organisasi belum memiliki peta risiko formal dan strategi mitigasi yang jelas, sehingga risiko cenderung ditangani secara reaktif. Fernandez et al. (2022) meneliti layanan internet di Indonesia dan menemukan bahwa governance maturity masih berada

di level rendah, tidak sesuai dengan indikator COBIT 2019. Temuan tersebut diperkuat oleh penelitian Fernandes Gamaliel et al. (2024) yang menunjukkan bahwa penggunaan form survei manajemen risiko SPBE di banyak instansi belum maksimal, sehingga tidak dapat berfungsi optimal sebagai instrumen monitoring dan evaluasi. Penelitian lain oleh Oktaviana et al. (2024) membuktikan bahwa COBIT 2019 relevan untuk digunakan pada perusahaan startup dalam mengevaluasi manajemen risiko, tetapi implementasi yang dilakukan masih terbatas dan belum mencapai level kapabilitas yang tinggi.

Hasil penelitian-penelitian terdahulu tersebut menegaskan adanya kesenjangan antara kondisi aktual dan kondisi ideal dalam penerapan manajemen risiko informasi Humaira et al., (2024). Kondisi aktual menunjukkan bahwa sebagian besar instansi pemerintah maupun organisasi di sektor teknologi informasi masih berada pada level kapabilitas rendah, di mana proses manajemen risiko sudah mulai dilakukan tetapi belum terdokumentasi, belum dievaluasi secara konsisten, dan belum terintegrasi dengan kebijakan organisasi secara menyeluruh Amali et al., (2023). Di sisi lain, kondisi ideal yang diharapkan adalah tercapainya tata kelola risiko yang sistematis, terdokumentasi dengan baik, serta dilaksanakan secara berkelanjutan sesuai standar nasional maupun internasional.

Kesenjangan ini bukan hanya menggambarkan lemahnya tata kelola risiko, tetapi juga menunjukkan adanya risiko nyata yang dapat menghambat keberlangsungan pelayanan publik berbasis elektronik Nyári & Kerti, (2024). Apabila hal ini tidak segera ditangani, maka dapat menimbulkan konsekuensi serius, seperti meningkatnya kerentanan terhadap serangan siber, terganggunya

layanan masyarakat, hilangnya data penting, bahkan menurunnya tingkat kepercayaan publik terhadap pemerintahan Fatayat, (2023). Oleh karena itu, perlunya penelitian lebih lanjut tidak hanya berorientasi pada aspek akademis, tetapi juga memiliki urgensi praktis untuk membantu instansi pemerintah daerah dalam memperbaiki sistem manajemen risiko Haddad, (2023). Dengan adanya evaluasi yang sistematis dan rekomendasi yang terarah, pemerintah daerah dapat lebih mudah menentukan prioritas perbaikan serta memastikan implementasi SPBE berjalan sesuai standar yang ditetapkan. Selain itu juga membantu memperbaiki kondisi yang ada.

Tabel 2. 6 Ringkasan Penelitian Terdahulu SPBE dan COBIT 2019

Peneliti & Tahun	Objek Penelitian	Domain COBIT	Level Kapabilitas	Temuan Utama
Sari & Juwairiah (2023)	DISKOMINFO Kabupaten Blitar	EDM03 & APO12	Level 2 (<i>Managed</i>)	Proses manajemen risiko ada, tetapi belum terdokumentasi dan dievaluasi.
Enrique & Fianty (2023)	Perusahaan Jasa TI di Indonesia	EDM03 & APO12	Level 1–2	Tidak ada peta risiko formal, strategi mitigasi masih lemah.
Fernandez et al. (2022)	Layanan Internet di Indonesia	Beberapa domain COBIT	Level 1–2	Governance maturity belum sesuai indikator COBIT 2019.
Fernandes Gamaliel et al. (2024)	Sistem Informasi ARKAS (Pendidikan)	APO12 & DSS04	Level 2 (<i>Managed</i>)	Pemanfaatan form survei risiko minim, evaluasi tidak optimal.

Oktaviana et al. (2024)	Startup Teknologi di Indonesia	APO12	Level 2–3	COBIT 2019 efektif untuk evaluasi risiko, tetapi implementasi masih rendah.
-------------------------	--------------------------------	-------	-----------	---

Berdasarkan beberapa penelitian terdahulu (Tabel 2.1), terlihat pola yang konsisten bahwa tingkat kapabilitas manajemen risiko informasi di berbagai instansi pemerintah maupun organisasi TI masih berada pada level rendah (Level 1–2). Kondisi ini menunjukkan bahwa proses manajemen risiko sudah mulai diterapkan, tetapi belum terdokumentasi secara konsisten dan belum terintegrasi dengan kebijakan organisasi secara menyeluruh. Hal inilah yang menjadi dasar urgensi penelitian ini untuk melakukan evaluasi kapabilitas manajemen risiko informasi SPBE pada Pemerintah Kabupaten Blitar menggunakan kerangka kerja COBIT 2019.

Secara keseluruhan, hasil-hasil penelitian terdahulu ini memperlihatkan bahwa ada pola yang konsisten, yaitu kapabilitas manajemen risiko informasi di Indonesia masih berada pada level rendah (Level 1–2), dengan kecenderungan belum adanya dokumentasi formal, kurangnya strategi mitigasi, serta minimnya mekanisme evaluasi berkelanjutan Haster & Hartomo, (2022). Kondisi inilah yang kemudian menjadi dasar urgensi penelitian, yakni melakukan evaluasi kapabilitas manajemen risiko informasi SPBE pada Pemerintah Kabupaten Blitar menggunakan kerangka COBIT 2019, dengan harapan dapat memberikan gambaran yang lebih jelas

Berdasarkan tinjauan pustaka yang telah dibahas, dapat disimpulkan

bahwa penelitian mengenai evaluasi kapabilitas manajemen risiko informasi SPBE dengan menggunakan COBIT 2019 memiliki dasar teoritis yang kuat. SPBE sebagai kebijakan nasional menuntut adanya pengelolaan risiko yang tidak hanya terstandarisasi, tetapi juga terukur dan terdokumentasi dengan baik Darmi et al., (2024). Sementara itu, penelitian-penelitian sebelumnya menunjukkan bahwa praktik pengelolaan risiko di berbagai instansi masih jauh dari ideal, baik dari sisi dokumentasi, pemetaan risiko, maupun mekanisme evaluasi berkelanjutan. Hal ini menegaskan bahwa penelitian dengan menggunakan COBIT 2019, khususnya pada domain EDM03, APO12 dan DSS04, sangat relevan untuk dilakukan. Hasil yang diperoleh tidak hanya akan memberikan gambaran mengenai tingkat kapabilitas risiko di Pemerintah Kabupaten Blitar, tetapi juga dapat menghasilkan rekomendasi strategis dan teknis yang berguna bagi penguatan SPBE secara menyeluruh Fianty & Brian, (2023). Dengan demikian, penelitian ini diharapkan mampu berkontribusi dalam menjembatani kesenjangan antara kondisi eksisting dan kondisi ideal. Penelitian ini tidak hanya menilai kondisi saat ini, tetapi juga memberikan arah yang jelas bagi peningkatan tata kelola risiko informasi agar penerapan SPBE dapat berjalan lebih optimal.

Tabel 2. 7 Perbandingan Standar Tata Kelola dan Manajemen Risiko Informasi

Standar/Framework	Fokus Utama	Lingkup	Kelebihan	Keterkaitan dengan Penelitian
COBIT 2019	Tata kelola & manajemen TI	Spesifik pada IT Governance, termasuk risiko informasi	Menyediakan domain, proses, dan level kapabilitas (0–5)	Digunakan sebagai framework utama untuk evaluasi kapabilitas manajemen risiko informasi SPBE
ISO 31000:2018	Manajemen risiko secara umum	Semua bidang (keuangan, operasional, TI, dll.)	Memberikan prinsip dan panduan umum dalam identifikasi, analisis, mitigasi risiko	Jadi acuan teori umum dalam pengelolaan risiko informasi
ISO/IEC 27001:2022	Keamanan informasi	Spesifik pada Information Security Management System (ISMS)	Fokus pada kerahasiaan, integritas, dan ketersediaan data	Jadi standar pendukung untuk aspek keamanan informasi SPBE

Berdasarkan Tabel 2.2 di atas, setiap standar memiliki peran yang saling melengkapi dalam pengelolaan risiko informasi. Dengan demikian, COBIT 2019 digunakan sebagai kerangka evaluasi utama dalam penelitian ini untuk menilai kapabilitas manajemen risiko informasi SPBE di Pemerintah Kabupaten Blitar.

Selain itu, perbandingan ini juga menegaskan posisi penelitian agar tidak hanya berfokus pada satu kerangka kerja, tetapi menggunakan pendekatan yang integratif. COBIT 2019 berperan sebagai instrumen utama untuk pengukuran kapabilitas, ISO 31000 memberikan landasan konseptual dalam proses manajemen

risiko, sedangkan ISO/IEC 27001 memperkuat aspek teknis keamanan informasi. Dengan demikian, ketiga standar tersebut menjadi dasar teoritis yang saling melengkapi, dan digunakan untuk memperkuat evaluasi kapabilitas manajemen risiko informasi dalam penelitian ini.

Penelitian ini memiliki kebaruan (*novelty*) dibandingkan penelitian terdahulu dalam beberapa aspek berikut:

1. **Objek Penelitian Spesifik** – Penelitian ini secara khusus mengevaluasi kapabilitas manajemen risiko informasi pada Sistem Pemerintahan Berbasis Elektronik (SPBE) Pemerintah Kabupaten Blitar, dengan fokus utama pada sistem e-Kinerja, yang belum pernah menjadi objek penelitian terdahulu.
2. **Pendekatan Integratif** – Berbeda dari penelitian sebelumnya yang hanya menggunakan satu standar (misalnya COBIT 2019 atau ISO 31000 saja), penelitian ini menggabungkan tiga standar internasional, yaitu COBIT 2019, ISO 31000:2018, dan ISO/IEC 27001:2022, untuk menghasilkan evaluasi yang lebih komprehensif.
3. **Penggunaan Sistem Digital Survey Risiko** – Penelitian ini tidak hanya bersifat teoretis, tetapi juga mengembangkan dan menguji aplikasi berbasis web “Survey Risiko” sebagai alat bantu untuk melakukan evaluasi kapabilitas secara otomatis, sehingga memperkenalkan pendekatan baru dalam pengukuran manajemen risiko SPBE di lingkungan pemerintahan daerah.
4. **Analisis Gap dan Rekomendasi Berbasis Domain COBIT 2019** – Penelitian ini menghasilkan analisis kesenjangan (*gap analysis*) antara kondisi aktual dan kondisi ideal serta menyusun rekomendasi peningkatan kapabilitas

berdasarkan domain EDM03, APO12, dan DSS04, yang disesuaikan dengan karakteristik instansi pemerintah daerah. Dengan kebaruan tersebut, penelitian ini diharapkan dapat berkontribusi dalam memperkaya kajian empiris tentang penerapan COBIT 2019 di sektor pemerintahan daerah sekaligus memberikan model evaluasi risiko SPBE yang lebih terukur dan dapat diimplementasikan secara praktis.

2.4 Manajemen Risiko dalam SPBE

Manajemen risiko merupakan suatu proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang dapat memengaruhi pencapaian tujuan organisasi Gheorghe Asachi Technical University of Iași, Romania et al., (2022). Dalam konteks penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE), manajemen risiko memiliki peranan penting dalam memastikan keberlangsungan layanan publik digital agar tetap aman, andal, dan terhindar dari gangguan yang dapat merugikan instansi maupun masyarakat. Menurut ISO 31000:2018, manajemen risiko adalah kegiatan terkoordinasi untuk mengarahkan dan mengendalikan organisasi dalam menghadapi risiko. Sementara berdasarkan Permenpan RB Nomor 5 Tahun 2020 tentang Manajemen Risiko SPBE, setiap instansi pemerintah diwajibkan untuk melaksanakan proses manajemen risiko yang meliputi tahapan: identifikasi risiko, analisis risiko, evaluasi risiko, serta perencanaan dan pelaksanaan mitigasi risiko.

Penerapan manajemen risiko dalam SPBE bertujuan untuk meminimalkan potensi ancaman seperti kebocoran data, kegagalan sistem, serangan siber, atau gangguan operasional yang dapat menghambat pelayanan publik berbasis digital. Melalui penerapan yang efektif, instansi pemerintah dapat meningkatkan keandalan

layanan, menjaga kerahasiaan dan integritas data, serta membangun kepercayaan publik terhadap sistem digital pemerintahan.

Dalam kerangka COBIT 2019, manajemen risiko dikaitkan dengan tiga domain utama, yaitu EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*) dan DSS04 (*Manage Continuity*). Domain EDM03 berfokus pada pengawasan strategis terhadap risiko agar tetap berada dalam tingkat yang dapat diterima oleh organisasi, dan APO12 menekankan pada pelaksanaan operasional manajemen risiko, mulai dari identifikasi hingga pemantauan risiko secara berkelanjutan, sedangkan DSS04 berfokus pada pengelolaan keberlanjutan layanan (*manage continuity*) yang memastikan sistem dan layanan SPBE tetap berjalan atau dapat segera dipulihkan apabila terjadi gangguan, kegagalan, atau insiden keamanan informasi. Integrasi antara COBIT 2019 dan ISO 31000 memungkinkan pengelolaan risiko SPBE dilakukan secara terstruktur, terdokumentasi, dan terukur sesuai dengan praktik terbaik internasional.

BAB III

DESAIN DAN IMPLEMENTASI

3.1 Desain Penelitian

Penelitian ini disusun dengan tujuan mengevaluasi kapabilitas manajemen risiko informasi pada penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) di Pemerintah Kabupaten Blitar dengan menggunakan kerangka kerja COBIT 2019. Fokus penelitian diarahkan pada domain EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*) dan DSS04 (*Manage Continuity*), karena ketiganya berkaitan langsung dengan pengelolaan risiko strategis maupun operasional dalam tata kelola TI. Desain penelitian yang dipilih bersifat deskriptif dengan pendekatan campuran kualitatif dan kuantitatif. Pendekatan deskriptif dipilih untuk menggambarkan kondisi nyata kapabilitas manajemen risiko berdasarkan observasi, kuesioner, wawancara, dan dokumentasi lapangan. Sementara itu, pendekatan kuantitatif digunakan untuk menghitung pencapaian tingkat kapabilitas pada setiap domain COBIT yang diteliti. Tahapan penelitian diawali dengan studi literatur terhadap regulasi, standar, dan kerangka kerja yang relevan, seperti Perpres Nomor 95 Tahun 2018 tentang SPBE, Permenpan-RB Nomor 5 Tahun 2020 tentang Manajemen Risiko SPBE, serta standar internasional ISO 31000:2018 dan ISO/IEC 27001:2022. Tahap ini penting untuk membangun landasan konseptual yang kokoh sebelum melakukan pengumpulan data lapangan.

Deskripsi dan Karakteristik Data Penelitian :

Data yang digunakan dalam penelitian ini terdiri atas dua jenis, yaitu data primer dan data sekunder, dengan karakteristik sebagai berikut:

Tabel 3.1 Deskripsi dan Karakteristik Data Penelitian

Jenis Data	Sumber Data	Metode Pengumpulan	Jumlah / Cakupan	Jenis Item / Skala
Data Primer	Dinas Komunikasi dan Informatika Kabupaten Blitar	Kuesioner berbasis indikator COBIT 2019 (EDM03, APO12, DSS04)	15 responden dari pejabat/staf yang terlibat dalam pengelolaan SPBE	15–20 butir pertanyaan dengan skala Likert 1–5
Data Primer (Pendukung)	Dinas Kominfo Kabupaten Blitar	Wawancara semi-terstruktur	3 narasumber (Kepala Bidang TI, staf pengelola e-Kinerja, dan analis SPBE)	Pertanyaan terbuka berdasarkan domain COBIT
Data Primer (Observasi)	Dinas Kominfo Kabupaten Blitar	Observasi langsung proses manajemen risiko SPBE dan dokumentasi sistem e-Kinerja	3 kali kunjungan lapangan	Catatan lapangan dan foto kegiatan observasi
Data Sekunder	Dokumen instansi dan sumber resmi pemerintah	Studi literatur dan dokumen pendukung	Dokumen SPBE, kebijakan keamanan informasi, laporan monev SPBE, dan laporan BSSN	Data tekstual dan laporan resmi

Penelitian ini menggunakan skala Likert (1–5) untuk mengukur tingkat penerapan indikator kapabilitas pada setiap domain COBIT 2019, dengan kriteria sebagai berikut:

1 = Sangat Tidak Setuju,

2 = Tidak Setuju,

3 = Cukup Setuju,

4 = Setuju,

5 = Sangat Setuju.

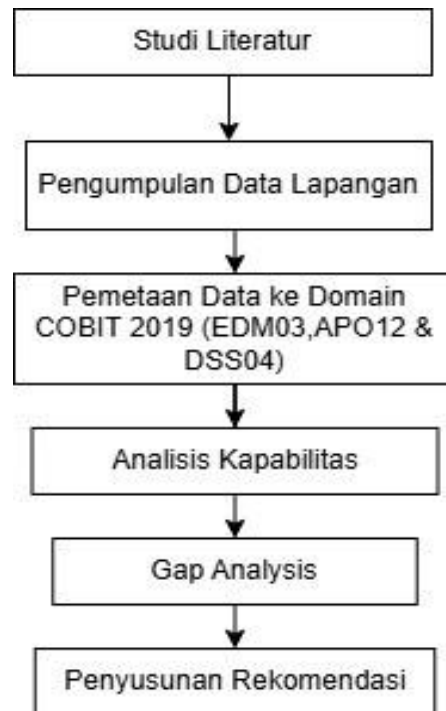
Dengan karakteristik tersebut, penelitian ini berfokus pada pengukuran kapabilitas manajemen risiko SPBE berdasarkan data aktual dari instansi terkait, yang kemudian diolah dan dianalisis untuk memperoleh nilai rata-rata tiap indikator dan menentukan level kapabilitas (Level 0–5).

Tahap berikutnya adalah pengumpulan data melalui penyebaran kuesioner kepada pihak yang terkait dengan pengelolaan SPBE, wawancara mendalam dengan pejabat dan staf Dinas Kominfo Kabupaten Blitar, serta observasi langsung terhadap aktivitas pengelolaan risiko yang sedang berjalan. Data yang diperoleh kemudian dipetakan ke dalam indikator kapabilitas COBIT 2019 untuk mengetahui sejauh mana implementasi manajemen risiko sudah dilakukan. Selanjutnya dilakukan analisis kapabilitas untuk mengidentifikasi level pencapaian, dilanjutkan dengan gap analysis untuk membandingkan kondisi aktual dengan kondisi ideal sesuai standar COBIT 2019. Dari proses ini diperoleh gambaran kesenjangan yang ada, yang kemudian menjadi dasar penyusunan rekomendasi strategis maupun teknis guna meningkatkan kapabilitas manajemen risiko informasi SPBE. Dengan desain penelitian yang sistematis ini, hasil yang diperoleh tidak hanya memberi deskripsi faktual tentang kondisi SPBE di Kabupaten Blitar, tetapi juga menawarkan solusi konkret yang dapat diterapkan untuk memperkuat tata kelola risiko informasi sesuai standar nasional dan internasional.

Dengan pendekatan ini, penelitian tidak hanya berhenti pada tahap

evaluasi, tetapi juga berfokus pada penyusunan langkah-langkah perbaikan yang dapat diimplementasikan secara nyata. Pendekatan analisis kesenjangan (*gap analysis*) membantu mengidentifikasi prioritas perbaikan yang harus dilakukan terlebih dahulu, sehingga rekomendasi yang dihasilkan lebih terarah dan sesuai dengan kebutuhan organisasi. Selain itu, keterlibatan langsung pejabat dan staf Dinas Kominfo Kabupaten Blitar memberikan nilai tambah karena rekomendasi yang disusun dapat langsung dikaitkan dengan kondisi lapangan, sehingga hasil penelitian lebih aplikatif dan berpotensi memberikan dampak nyata terhadap peningkatan kapabilitas manajemen risiko informasi SPBE.

Penggunaan framework COBIT 2019 dalam penelitian ini memberikan struktur yang jelas dalam menilai kapabilitas organisasi. Setiap domain yang dievaluasi memiliki indikator kapabilitas tersendiri, mulai dari perencanaan, pelaksanaan, hingga pengawasan. Hal ini memungkinkan peneliti untuk memperoleh gambaran yang lebih detail mengenai kekuatan maupun kelemahan dari tata kelola yang sedang berjalan. Dengan demikian, hasil penelitian tidak hanya berupa penilaian umum, tetapi juga mampu menunjukkan aspek spesifik yang memerlukan perhatian lebih dari pihak pengelola SPBE.



Gambar 3. 1 Desain Penelitian

Gambar 3.1 tersebut menggambarkan alur penelitian yang dilakukan secara sistematis mulai dari tahapan awal hingga akhir. Tahap pertama adalah studi literatur, yaitu mempelajari berbagai regulasi, standar, dan kerangka kerja yang relevan seperti Perpres Nomor 95 Tahun 2018 tentang SPBE, Permenpan-RB Nomor 5 Tahun 2020, ISO 31000:2018, ISO/IEC 27001:2022, serta COBIT 2019.

Tahap kedua adalah pengumpulan data lapangan melalui kuesioner, wawancara, observasi, dan analisis dokumen, yang bertujuan memperoleh informasi terkait kondisi nyata manajemen risiko SPBE di Pemerintah Kabupaten Blitar. Data yang diperoleh kemudian dipetakan ke dalam domain COBIT 2019 (EDM03, APO12 & DSS04) untuk mengetahui kesesuaian dengan indikator kapabilitas yang ditentukan.

Tahap selanjutnya adalah analisis kapabilitas, di mana hasil pemetaan diukur berdasarkan level kapabilitas COBIT 2019. Setelah itu dilakukan gap analysis, yaitu membandingkan antara kondisi aktual dengan kondisi ideal untuk mengidentifikasi kesenjangan yang ada. Tahap terakhir adalah penyusunan rekomendasi, baik strategis maupun teknis, yang dapat digunakan oleh Pemerintah Kabupaten Blitar sebagai upaya perbaikan dalam meningkatkan kapabilitas manajemen risiko informasi SPBE. Dengan alur ini, penelitian diharapkan dapat memberikan gambaran menyeluruh sekaligus solusi konkret terhadap permasalahan yang ditemukan.

3.2 Tahapan Penelitian

Adapun tahapan penelitian ini terdiri atas beberapa langkah utama, yaitu:

1. Studi Literatur

Tahap ini dilakukan untuk memperoleh landasan teori yang kuat mengenai konsep dan praktik manajemen risiko informasi dalam penerapan SPBE.

Peneliti mempelajari berbagai regulasi dan standar, seperti:

- a. **COBIT 2019**, sebagai framework utama tata kelola TI,
- b. **ISO 31000:2018**, sebagai pedoman manajemen risiko,
- c. **ISO/IEC 27001:2022**, untuk keamanan informasi, serta
- d. **Peraturan Presiden Nomor 95 Tahun 2018** tentang SPBE.

Tujuan studi literatur ini adalah mengidentifikasi indikator, prinsip, dan domain yang relevan agar penelitian memiliki dasar konseptual yang jelas serta selaras dengan praktik tata kelola TI yang diakui secara nasional dan internasional. Hasil tahap ini menjadi dasar dalam menyusun instrumen penelitian (kuesioner,

wawancara, dan observasi) sesuai dengan domain EDM03, APO12, dan DSS04 dari COBIT 2019.

2. Perancangan Instrumen Penelitian

Pada tahap ini, peneliti menyusun instrumen berupa kuesioner, pedoman wawancara, dan lembar observasi. Instrumen disusun berdasarkan indikator kapabilitas COBIT 2019, yaitu EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan DSS04 (*Manage Continuity*).

Responden dan Narasumber Penelitian

Kuesioner disebarkan kepada 15 responden yang terdiri atas pejabat dan staf Dinas Komunikasi dan Informatika Kabupaten Blitar yang terlibat langsung dalam pengelolaan Sistem Pemerintahan Berbasis Elektronik (SPBE), meliputi bidang TIK, e-Government, dan keamanan informasi.

Wawancara dilakukan terhadap 3 narasumber utama, yaitu:

1. Kepala Bidang TIK Dinas Kominfo Kabupaten Blitar,
2. Staf Pengelola Sistem e-Kinerja,
3. Analis SPBE.

a. Kuesioner

Kuesioner menggunakan skala **Likert 1–5**, dengan 1 = sangat tidak setuju dan 5 = sangat setuju.

Jumlah pertanyaan: 15 butir, dibagi menurut domain.

Tabel 3.2. Ringkasan Pertanyaan dan Hasil Rata-Rata Skor Kuesioner per Domain COBIT 2019

Domain	Indikator	Pertanyaan	Rata-rata Skor

EDM03	Penetapan Toleransi Risiko	“Apakah organisasi telah menetapkan tingkat toleransi risiko TI secara formal?”	
APO12	Analisis Risiko	“Apakah risiko SPBE telah dianalisis berdasarkan dampak dan kemungkinan terjadinya?”	
DSS04	Rencana Keberlangsungan Layanan	“Apakah terdapat rencana keberlangsungan layanan TI (BCP) yang diperbarui secara berkala?”	

Evaluasi Kapabilitas Manajemen Risiko Informasi SPBE

Kerangka Acuan: COBIT 2019 (Domain EDM03, APO12, DSS04)

Objek Penelitian: Dinas Komunikasi dan Informatika Kabupaten Blitar

Petunjuk Pengisian: Berilah tanda centang (✓) pada kolom yang sesuai dengan

pendapat Anda terhadap setiap pernyataan berikut:

Tabel 3.3 Skala Penilaian Responden

Skor	Keterangan
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Cukup Setuju
4	Setuju
5	Sangat Setuju

A. DOMAIN EDM03 – Ensure Risk Optimization

Tabel 3.4 Instrumen Penilaian Domain EDM03 COBIT 2019

No	Pernyataan	1	2	3	4	5
EDM03.01 – Evaluasi Risiko						
1	Organisasi telah menetapkan tingkat toleransi risiko TI secara formal dan terdokumentasi.					
2	Evaluasi risiko TI dilakukan secara berkala untuk menilai kesesuaian terhadap tujuan organisasi.					
3	Manajemen puncak terlibat aktif dalam proses pengambilan keputusan terkait risiko TI.					

4	Terdapat kebijakan tertulis mengenai tata kelola risiko dalam layanan SPBE.					
EDM03.02 – Optimasi Risiko						
5	Risiko TI dikaitkan langsung dengan sasaran strategis SPBE.					
6	Sumber daya dan anggaran disediakan untuk kegiatan mitigasi risiko TI.					
7	Tanggung jawab pengelolaan risiko TI sudah ditetapkan secara jelas di tiap unit kerja.					
EDM03.03 – Pemantauan Risiko						
8	Pimpinan menerima laporan risiko TI secara rutin dan terdokumentasi.					
9	Hasil evaluasi risiko digunakan sebagai dasar perbaikan sistem SPBE.					
10	Audit internal terhadap manajemen risiko dilakukan secara periodik.					

- a. Apakah organisasi telah menetapkan tingkat toleransi risiko TI secara formal?
- b. Apakah risiko TI telah dievaluasi untuk memastikan keselarasan dengan tujuan strategis organisasi?
- c. Apakah dilakukan pemantauan rutin terhadap risiko-risiko utama TI?

B. DOMAIN APO12 – Manage Risk

Tabel 3.5 Instrumen Penilaian Domain APO12 COBIT 2019

No	Pernyataan	1	2	3	4	5
APO12.01 – Kerangka Manajemen Risiko						
11	Instansi memiliki kebijakan formal tentang manajemen risiko SPBE.					
12	Proses manajemen risiko telah ditetapkan dan dikomunikasikan ke seluruh unit kerja.					
APO12.02 – Identifikasi Risiko						

13	Organisasi memiliki daftar risiko TI yang diidentifikasi secara berkala.					
14	Proses identifikasi risiko mencakup aspek teknis, operasional, dan keamanan informasi.					
APO12.03 – Analisis Risiko						
15	Risiko yang teridentifikasi dianalisis berdasarkan dampak dan kemungkinan terjadinya.					
16	Analisis risiko dilakukan dengan metode atau matriks tertentu (misal: skoring, heatmap).					
APO12.04 – Penanganan Risiko						
17	Rencana mitigasi risiko disusun dan diimplementasikan oleh unit kerja terkait.					
18	Efektivitas pengendalian risiko dievaluasi secara berkala.					
19	Hasil mitigasi risiko dilaporkan kepada pimpinan untuk ditindaklanjuti.					
APO12.05 – Pemantauan dan Pelaporan Risiko						
20	Pelaporan risiko SPBE dilakukan secara teratur dan didokumentasikan.					
21	Evaluasi hasil risiko menjadi bahan dalam penyusunan kebijakan TI berikutnya.					

- a. Apakah organisasi memiliki prosedur untuk mengidentifikasi risiko TI dan SPBE secara berkala?
- b. Apakah risiko yang telah diidentifikasi dianalisis berdasarkan dampak dan probabilitasnya?
- c. Apakah tersedia rencana mitigasi atau pengendalian terhadap risiko TI yang signifikan?
- d. Apakah hasil analisis risiko dikomunikasikan kepada pimpinan atau pihak

terkait?

C. DOMAIN DSS04 – Manage Continuity

Tabel 3.6 Instrumen Penilaian Domain DSS04 COBIT 2019

No	Pernyataan	1	2	3	4	5
DSS04.01 – Perencanaan Keberlanjutan						
22	Organisasi memiliki dokumen rencana keberlangsungan layanan (Business Continuity Plan / BCP).					
23	Rencana keberlanjutan tersebut mencakup langkah pemulihan data dan sistem SPBE.					
DSS04.02 – Uji Coba dan Pemulihan Sistem						
24	Uji coba pemulihan sistem (disaster recovery test) dilakukan minimal sekali dalam setahun.					
25	Hasil uji coba dan evaluasi pemulihan sistem didokumentasikan.					
DSS04.03 – Pemeliharaan Rencana Keberlanjutan						
26	Rencana keberlanjutan diperbarui setiap terjadi perubahan besar dalam infrastruktur TI.					
27	Terdapat petugas khusus yang bertanggung jawab terhadap pemeliharaan sistem dan data cadangan.					
28	Evaluasi pasca insiden digunakan untuk memperbaiki sistem keberlanjutan layanan.					

- a. Apakah organisasi memiliki dokumen formal rencana keberlangsungan layanan TI?
- b. Apakah dilakukan simulasi atau uji coba pemulihan sistem pascakegagalan?
- c. Apakah rencana keberlangsungan bisnis diperbarui secara berkala

sesuai perubahan sistem?

b. Pedoman Wawancara pertanyaan wawancara:

1. “Apakah instansi memiliki dokumen formal terkait penetapan risiko TI?”
2. “Bagaimana proses identifikasi dan mitigasi risiko dilakukan?”
3. “Apakah dilakukan pemantauan rutin terhadap risiko layanan digital?”

Temuan ini menguatkan hasil kuesioner bahwa kapabilitas manajemen risiko SPBE masih berada pada Level 2 (Managed) dan perlu peningkatan dokumentasi serta standarisasi proses.

c. Observasi Lapangan

Observasi dilakukan secara langsung di lingkungan kerja Dinas Komunikasi dan Informatika Kabupaten Blitar untuk memahami bagaimana proses manajemen risiko informasi diterapkan dalam praktik sehari-hari, khususnya pada sistem e- Kinerja.

Kegiatan observasi mencakup:

- a. **Pengamatan terhadap aktivitas operasional sistem e-Kinerja**, meliputi proses login pengguna, input data kinerja ASN, serta mekanisme penyimpanan dan akses data.
- b. **Pengamatan terhadap pelaksanaan identifikasi risiko**, yaitu bagaimana staf melakukan pencatatan risiko, menentukan kategori risiko, serta proses pelaporan risiko ke atasan.
- c. **Pengamatan terhadap koordinasi antar-bidang**, terutama antara tim pengelola TI dan bidang e-Government dalam menangani gangguan sistem atau potensi kebocoran data.

- d. **Verifikasi terhadap keberadaan dokumen dan sistem pendukung**, seperti daftar risiko, rencana mitigasi, dan laporan hasil evaluasi risiko SPBE.

Hasil observasi menunjukkan bahwa sebagian proses pengelolaan risiko sudah berjalan, seperti pencatatan risiko operasional. Namun, kegiatan monitoring dan evaluasi risiko belum dilakukan secara terjadwal dan dokumentasi formalnya masih terbatas. Selain itu, komunikasi risiko antar- bidang belum terintegrasi dalam satu sistem informasi yang baku.

Dari kegiatan observasi lapangan tersebut, informasi yang berhasil diperoleh meliputi beberapa aspek penting berikut:

- a. **Kondisi aktual penerapan manajemen risiko SPBE** — terlihat bahwa proses identifikasi dan pelaporan risiko sudah dilakukan, tetapi belum berjalan secara sistematis di semua bidang.
- b. **Tingkat keterlibatan pegawai** — ditemukan bahwa sebagian staf sudah memahami prosedur risiko, namun belum semua mengikuti memiliki peran yang jelas dalam mitigasi risiko.
- c. **Kelengkapan dan konsistensi dokumentasi** — dokumen seperti daftar risiko, tetapi belum diperbarui secara berkala dan belum tersimpan dalam satu sistem terintegrasi.
- d. **Koordinasi antarbidang** — koordinasi dalam pengelolaan risiko masih bersifat manual melalui rapat atau komunikasi informal, belum terotomasi dalam platform SPBE.
- e. **Kesiapan sistem e-Kinerja** — sistem sudah berjalan baik dalam

fungsionalitas, namun belum dilengkapi mekanisme kontrol risiko seperti deteksi dini gangguan atau keamanan data. Jadi, informasi utama yang diperoleh dari observasi adalah gambaran nyata mengenai sejauh mana manajemen risiko informasi SPBE telah diterapkan, mencakup praktik, kendala, dan kesenjangan antara kondisi aktual dan standar ideal yang diacu dalam COBIT 2019 (EDM03, APO12, DSS04).

4. Analisis Kapabilitas

Tahapan analisis kapabilitas dilakukan untuk menilai sejauh mana tingkat kematangan (capability level) proses manajemen risiko informasi SPBE di Dinas Kominfo Kabupaten Blitar berdasarkan kerangka kerja **COBIT 2019**. Analisis ini dilakukan dengan langkah-langkah sistematis sebagai berikut:

1. Pengolahan Data Kuesioner

Setiap responden memberikan penilaian terhadap pernyataan pada kuesioner dengan menggunakan skala Likert 1–5, di mana:

- a. 1 = Tidak dilakukan sama sekali,
- b. 2= Dilakukan sebagian tetapi tidak konsisten,
- c. 3= Sudah dilakukan dan terdokumentasi sebagian,
- d. 4= Sudah dilakukan, terdokumentasi, dan dievaluasi secara berkala,
- e. 5= Sudah dilakukan secara menyeluruh, terintegrasi, dan terus ditingkatkan.

Nilai dari seluruh responden untuk setiap indikator dijumlahkan dan dihitung rata-ratanya, sehingga diperoleh skor representatif tiap proses (misalnya EDM03.01, APO12.02, dan DSS04.01).

2. Pemetaan ke Level Kapabilitas COBIT 2019

Skor rata-rata yang diperoleh kemudian dipetakan ke dalam tingkat kapabilitas (Capability Level) COBIT 2019, dengan kriteria berikut:

- 2.1 Level 0 (Incomplete)** – Proses belum dijalankan.
- 2.2 Level 1 (Performed)** – Proses dijalankan tetapi belum terstruktur.
- 2.3 Level 2 (Managed)** – Proses dijalankan dan sudah dikelola, namun belum terdokumentasi secara formal.
- 2.4 Level 3 (Established)** – Proses sudah terdokumentasi dan diterapkan secara konsisten.
- 2.5 Level 4 (Predictable)** – Proses diukur dan dikendalikan secara kuantitatif.
- 2.6 Level 5 (Optimizing)** – Proses terus diperbaiki berdasarkan hasil evaluasi dan inovasi.

Berdasarkan hasil pengolahan data, sebagian besar domain — EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan DSS04 (*Manage Continuity*) — memperoleh skor rata-rata antara 2,3–2,6, yang dikategorikan pada Level 2 (*Managed Process*).

3. Interpretasi Hasil Analisis

Level 2 menunjukkan bahwa proses manajemen risiko informasi sudah berjalan di lingkungan Dinas Kominfo Kabupaten Blitar, namun belum sepenuhnya terdokumentasi dan belum dilakukan evaluasi formal secara berkala. Hal ini terlihat dari hasil wawancara, di mana staf menyatakan bahwa kegiatan identifikasi dan mitigasi risiko telah dilakukan, tetapi panduan resmi

dan mekanisme monitoring belum diformalkan dalam dokumen kebijakan.

4. Kesimpulan Analisis Kapabilitas

Berdasarkan analisis, dapat disimpulkan bahwa tingkat kapabilitas manajemen risiko informasi SPBE masih berada pada Level 2 (*Managed*). Kondisi ini menunjukkan adanya kesadaran dan praktik dasar pengelolaan risiko, tetapi belum terukur secara sistematis serta belum memiliki standar dokumentasi dan evaluasi berkelanjutan sebagaimana disarankan dalam COBIT 2019.

Hasil analisis ini menjadi dasar untuk tahap selanjutnya, yaitu Analisis Gap dan Rekomendasi, guna mengidentifikasi kesenjangan antara kondisi aktual dan kondisi ideal serta menyusun langkah perbaikan yang tepat.

5. Analisis Gap dan Rekomendasi

Analisis gap merupakan tahapan untuk mengidentifikasi kesenjangan antara kondisi aktual hasil penelitian dengan kondisi ideal yang diharapkan berdasarkan standar COBIT 2019. Tujuannya adalah mengetahui aspek mana yang masih perlu diperbaiki agar tingkat kapabilitas manajemen risiko informasi SPBE dapat meningkat ke level yang lebih tinggi.

Langkah-langkah analisis dilakukan sebagai berikut:

1. Menentukan Kondisi Aktual

Berdasarkan hasil analisis kapabilitas pada tahap sebelumnya, rata-rata nilai manajemen risiko informasi SPBE di Dinas Kominfo Kabupaten Blitar berada pada Level 2 (*Managed Process*). Artinya, proses manajemen risiko telah berjalan, tetapi belum terdokumentasi secara formal, belum memiliki mekanisme pengukuran yang jelas, dan pelaksanaannya belum

konsisten di seluruh bidang.

2. **Menetapkan Kondisi Ideal**

Berdasarkan pedoman COBIT 2019, kondisi ideal yang diharapkan berada pada Level 3 (*Established Process*). Pada level ini, proses manajemen risiko harus sudah:

- a. Memiliki panduan tertulis atau SOP yang jelas dan disetujui pimpinan,
- b. Diterapkan secara konsisten di seluruh unit kerja,
- c. Terdokumentasi dan dapat diaudit,
- d. Didukung dengan pengukuran kinerja dan evaluasi periodik untuk memastikan efektivitasnya.

3. **Membandingkan Kondisi Aktual dan Ideal (Gap Analysis)**

Perbandingan antara kondisi aktual dan ideal dilakukan dengan menilai setiap domain COBIT 2019 yang digunakan dalam penelitian, yaitu EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan DSS04 (*Manage Continuity*).

a. Domain EDM03 – Ensure Risk Optimization

3.1 *Kondisi Aktual*: Evaluasi risiko TI sudah dilakukan secara berkala, namun hasilnya belum didokumentasikan secara sistematis dan belum menjadi dasar pengambilan keputusan strategis.

3.2 *Kondisi Ideal*: Evaluasi risiko dilakukan secara terukur dan terdokumentasi, serta menjadi dasar dalam penyusunan kebijakan SPBE.

3.3 *Gap*: Belum adanya format laporan risiko yang baku dan mekanisme

pelaporan ke pimpinan.

3.4 *Rekomendasi*: Membuat dokumen Risk Register SPBE yang mencatat seluruh risiko beserta tingkat dampak dan rencana mitigasinya.

b. Domain APO12 – Manage Risk

- a. *Kondisi Aktual*: Identifikasi dan penilaian risiko dilakukan, namun belum diatur dalam SOP formal.
- b. *Kondisi Ideal*: Proses manajemen risiko dijalankan berdasarkan pedoman tertulis dengan tanggung jawab yang jelas.
- c. *Gap*: Belum ada dokumen kebijakan atau prosedur resmi tentang manajemen risiko SPBE.
- d. *Rekomendasi*: Menyusun SOP Manajemen Risiko SPBE, termasuk tahapan identifikasi, analisis, evaluasi, mitigasi, dan pemantauan risiko.

c. Domain DSS04 – Manage Continuity

- a. *Kondisi Aktual*: Dinas Kominfo memiliki mekanisme pemulihan data dan backup sistem, namun belum dilakukan simulasi uji pemulihan secara rutin.
- b. *Kondisi Ideal*: Proses kesinambungan layanan diuji secara berkala dan hasilnya dilaporkan serta diperbarui.
- c. *Gap*: Belum adanya jadwal uji coba pemulihan sistem (*disaster recovery test*) dan dokumentasi hasilnya.
- d. *Rekomendasi*: Menetapkan jadwal uji pemulihan sistem minimal dua kali setahun dan membuat laporan hasil uji untuk evaluasi

perbaikan.

4. Analisis Kesenjangan Umum (*Gap Summary*)

Dari hasil perbandingan seluruh domain, diperoleh tiga area utama yang masih lemah:

- a. **Dokumentasi dan Kebijakan:** Belum ada SOP formal, risk register, serta panduan evaluasi risiko SPBE.
- b. **Monitoring dan Audit:** Belum dilakukan pemantauan risiko secara periodik serta audit internal terhadap efektivitas manajemen risiko.
- c. **Kompetensi SDM:** Pengetahuan staf terkait manajemen risiko dan keamanan informasi masih terbatas.

5. Rekomendasi Umum dan Teknis

Berdasarkan analisis gap tersebut, rekomendasi yang disusun meliputi:

- a. **Membentuk Tim Manajemen Risiko SPBE** di bawah koordinasi Dinas Kominfo untuk mengelola risiko lintas bidang.
- b. **Menyusun SOP dan Panduan Risiko SPBE** sesuai dengan domain COBIT 2019, ISO 31000, dan Permenpan RB No. 5 Tahun 2020.
- c. **Melaksanakan pelatihan rutin** tentang manajemen risiko dan keamanan informasi bagi pegawai TI dan operator sistem SPBE.
- d. **Melakukan audit internal tahunan** terhadap efektivitas penerapan risiko SPBE.
- e. **Mengimplementasikan aplikasi “Survey Risiko Digital”** yang dikembangkan peneliti untuk mendukung evaluasi otomatis, dokumentasi hasil survei, dan pelaporan berbasis data real-time.

Maka, hasil analisis menunjukkan bahwa untuk mencapai Level 3 (*Established Process*), instansi perlu memperkuat dokumentasi, meningkatkan konsistensi penerapan, serta membangun sistem monitoring yang berkelanjutan. Implementasi rekomendasi ini diharapkan mampu meningkatkan kapabilitas manajemen risiko informasi SPBE secara terukur dan berkesinambungan.

5. Validasi dan Eksperimen

Tahap akhir penelitian adalah validasi melalui uji coba sistem aplikasi *Survey Risiko* yang dikembangkan peneliti. Uji dilakukan dengan 15 responden dari Dinas Kominfo. Hasil eksperimen menunjukkan bahwa:

- a. Semua responden berhasil mengisi kuesioner secara online tanpa kendala.
- b. Hasil perhitungan otomatis sistem 100% sama dengan hasil manual.
- c. 93% responden menyatakan tampilan dashboard mudah dipahami.
- d. Data tersimpan aman di Firestore meskipun koneksi sempat tidak stabil.

Temuan ini menunjukkan bahwa sistem *Survey Risiko* valid, akurat, dan layak diterapkan untuk evaluasi berkelanjutan di lingkungan SPBE Pemerintah Kabupaten Blitar.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Deskripsi Objek dan Responden Penelitian

Penelitian ini dilakukan pada Dinas Komunikasi dan Informatika Kabupaten Blitar, yaitu instansi pemerintahan yang memiliki tugas menyelenggarakan layanan Teknologi Informasi dan Komunikasi (TIK), pengelolaan Sistem Pemerintahan Berbasis Elektronik (SPBE), layanan data, keamanan informasi, serta infrastruktur jaringan di lingkungan Pemerintah Kabupaten Blitar. Salah satu layanan digital utama yang dikelola oleh Dinas Kominfo adalah sistem e-Kinerja, yaitu aplikasi yang digunakan oleh seluruh ASN untuk mencatat, mengelola, dan melaporkan kinerja harian maupun tahunan secara elektronik. Sistem ini bersifat kritis karena mempengaruhi proses penilaian kinerja pegawai, kedisiplinan, serta pelaporan kinerja instansi, sehingga gangguan atau risiko pada layanan ini dapat berdampak langsung terhadap efektivitas penyelenggaraan pemerintahan.

Analisis disusun berdasarkan hasil pengumpulan data yang diperoleh melalui penyebaran kuisisioner dan pelaksanaan wawancara kepada responden di Dinas Komunikasi dan Informatika Kabupaten Blitar. Kuisisioner digunakan untuk mengetahui tingkat penerapan manajemen risiko secara umum, sedangkan wawancara digunakan untuk memperoleh informasi mengenai praktik pengelolaan risiko. Seluruh hasil yang diperoleh kemudian dianalisis dan disesuaikan dengan kerangka kerja COBIT 2019, khususnya pada domain EDM03 (Ensure Risk Optimization), APO12 (Manage Risk), dan DSS04 (Manage Continuity). Sebagai

sistem yang digunakan secara intensif setiap hari, e-Kinerja memiliki berbagai risiko, seperti risiko kegagalan akses, ketidakakuratan data, ancaman keamanan informasi, hingga potensi downtime layanan. Oleh karena itu, penelitian ini berfokus untuk mengevaluasi manajemen risiko SPBE pada layanan e-Kinerja dengan menggunakan standar COBIT 2019. Dari keseluruhan kerangka COBIT 2019, penelitian ini secara khusus memilih tiga domain yang paling relevan, yaitu EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan DSS04 (*Manage Continuity*).

- a. Domain EDM03 dipilih karena terkait dengan peran pimpinan dalam menetapkan toleransi risiko, mengoptimalkan pengelolaan risiko, serta memastikan risiko berada pada tingkat yang dapat diterima
- b. Domain APO12 dipilih karena berhubungan dengan proses identifikasi, penilaian, dan mitigasi risiko operasional terhadap sistem e-Kinerja.
- c. Domain DSS04 dipilih karena berfokus pada keberlanjutan layanan (*continuity*), termasuk rencana pemulihan bencana, backup data, dan mekanisme tanggap darurat apabila terjadi gangguan layanan SPBE.

Ketiga domain tersebut saling melengkapi untuk memberikan gambaran menyeluruh mengenai bagaimana manajemen risiko SPBE dilaksanakan di Dinas Kominfo Kabupaten Blitar.

Metode pengumpulan data dalam penelitian ini dilakukan dengan tiga pendekatan utama. Pertama, pengisian kuisisioner COBIT 2019 yang disusun berdasarkan 17 pernyataan sesuai tiga domain yang diteliti (5 pernyataan EDM03, 7 pernyataan APO12, dan 5 pernyataan DSS04). Kuisisioner diberikan kepada 11

responden yang terlibat dalam pengelolaan, penggunaan, atau pengawasan layanan e-Kinerja. Setiap responden memberikan jawaban dari pertanyaan kuisisioner dan wawancara di setiap domain untuk menggambarkan tingkat kesesuaian praktik yang berjalan dengan standar COBIT 2019. Kedua, dilakukan dengan menunjukkan bukti sesuai apa tidak dengan pertanyaan atau alasan pada wawancara dan kuisisioner untuk setiap domain. Wawancara ini bertujuan untuk mengetahui secara lebih detail bagaimana pimpinan, staf teknis, dan unit terkait memahami, melaksanakan, serta berkoordinasi dalam proses pengelolaan risiko pada layanan e-Kinerja. bukti dari wawancara dan kuisisioner juga digunakan untuk memastikan apakah hasilnya konsisten dengan kondisi sebenarnya dan hasil wawancaranya.

Ketiga, dilakukan observasi dan pembuktian dokumen, seperti SOP keamanan informasi (jika tersedia). Observasi dokumen ini digunakan sebagai pembandingan untuk memvalidasi hasil kuisisioner dan wawancara. Dan tujuannya untuk menentukan skala Likert 1-5 didalam COBIT 2019.

Seluruh hasil jawaban yang terkumpul kemudian dianalisis, dan hasil skala Likert 1-5 dihitung nilai rata-rata pada setiap pernyataan kuisisioner, menentukan nilai rata-rata per domain, dan memetakan hasilnya ke dalam level kapabilitas COBIT 2019. Setelah itu, menghasilkan tingkat kematangan keseluruhan sehingga muncul gambaran interpretasi dan rekomendasi mengenai total rata-rata dan hasil level akhir pada layanan e-Kinerja di Dinas Kominfo Kabupaten Blitar.

A. Identifikasi Risiko pada Sistem e-Kinerja

Berdasarkan hasil observasi, wawancara, dan analisis, proses identifikasi risiko

pada sistem e-Kinerja dilakukan dengan memetakan kejadian, penyebab, dan dampak risiko yang berpotensi menghambat pencapaian tujuan organisasi. Identifikasi risiko melibatkan berbagai pihak, seperti tim teknis aplikasi, koordinator keamanan informasi, serta unit kepegawaian.

Metode identifikasi risiko dilakukan melalui:

1. Wawancara dengan stakeholder terkait

Observasi langsung terhadap sistem e-Kinerja

Adapun risiko-risiko utama yang teridentifikasi pada sistem e-Kinerja meliputi:

- a. Risiko kegagalan akses sistem (system downtime) yang dapat terjadi akibat gangguan jaringan atau server
- b. Risiko kehilangan atau kerusakan data, yang dapat disebabkan oleh kesalahan sistem atau kegagalan penyimpanan
- c. Risiko kebocoran data ASN, yang berpotensi terjadi akibat lemahnya pengamanan akses atau serangan siber
- d. Risiko kesalahan input data oleh pengguna, yang disebabkan oleh kurangnya pemahaman pengguna atau human error
- e. Risiko serangan siber , seperti malware atau peretasan yang dapat mengganggu sistem
- f. Risiko ketergantungan pada sistem lama , yang dapat menghambat pengembangan dan meningkatkan potensi gangguan

Identifikasi risiko ini diperoleh berdasarkan hasil observasi dan wawancara dengan pihak terkait di Dinas Kominfo Kabupaten Blitar. Hasil Identifikasi ini

menjadi dasar dalam proses analisis dan mitigasi risiko pada tahap selanjutnya.

B. Evaluasi Kapabilitas Proses Manajemen Risiko pada Sistem e-Kinerja:

Manajemen risiko pada e-Kinerja dilakukan secara sistematis melalui perencanaan, identifikasi, analisis (kualitatif dan kuantitatif), penentuan respon, mitigasi, hingga monitoring, di mana setiap tahap memiliki metode dan praktik yang jelas seperti wawancara, observasi, penggunaan matriks risiko, serta evaluasi berkala.

1. Hasil evaluasi menunjukkan bahwa perencanaan manajemen risiko pada sistem e-Kinerja dilakukan dengan menetapkan pendekatan, metode, proses, serta pihak yang terlibat dalam pengelolaan risiko. Proses ini mencakup penentuan mekanisme identifikasi risiko melalui wawancara dan observasi, penggunaan matriks risiko sebagai metode analisis, serta penentuan peran pihak terkait seperti tim teknis, koordinator keamanan informasi, dan unit kepegawaian. Selain itu, perencanaan juga mencakup penetapan langkah-langkah pengendalian risiko dan mekanisme monitoring yang akan digunakan. Meskipun demikian, perencanaan ini belum sepenuhnya terdokumentasi dalam bentuk dokumen formal seperti risk management plan yang terstruktur.

Berdasarkan transkrip wawancara, salah satu responden menyatakan:

“Dalam pelaksanaan manajemen risiko pada e-Kinerja, biasanya dilakukan diskusi dengan tim teknis dan unit terkait untuk menentukan langkah penanganan risiko serta cara pemantauannya” (Responden 1, Wawancara, Transkrip W4, Lampiran

A).

Responden lain juga menyatakan:

“Perencanaan risiko belum dibuat dalam dokumen khusus, tetapi masih berupa kesepakatan dan koordinasi antar unit ketika ada masalah” (Responden 4, Wawancara, Transkrip W5, Lampiran A).

Berdasarkan hasil wawancara, dapat dinilai bahwa perencanaan manajemen risiko pada sistem e-Kinerja sudah dilakukan melalui koordinasi dan diskusi antar unit yang terlibat, terutama antara tim teknis dan unit terkait dalam menentukan langkah penanganan serta pemantauan risiko. Namun, dari sisi dokumentasi, perencanaan tersebut belum memiliki standar formal dalam bentuk dokumen risk management plan, sehingga masih bersifat informal dan berbasis kesepakatan saat terjadi masalah. Dengan demikian, tingkat kapabilitas perencanaan manajemen risiko dapat dikategorikan sudah berjalan tetapi belum terstandarisasi secara penuh.

Proses perencanaan manajemen risiko dilakukan dengan tahapan awal berupa koordinasi dan diskusi antar pihak terkait untuk menentukan pendekatan, metode, serta pembagian peran dalam pengelolaan risiko. Selanjutnya ditetapkan mekanisme identifikasi risiko melalui wawancara dan observasi, serta metode analisis menggunakan matriks risiko. Setelah itu, ditentukan langkah-langkah pengendalian dan mekanisme monitoring yang akan digunakan. Hasil dari proses perencanaan ini kemudian menjadi acuan dalam pelaksanaan manajemen risiko pada sistem e-Kinerja, meskipun belum terdokumentasi secara formal dalam bentuk dokumen terstruktur.

2. Hasil evaluasi menunjukkan bahwa identifikasi risiko dilakukan melalui wawancara, observasi sistem , serta analisis terhadap potensi gangguan yang dapat mempengaruhi layanan e-Kinerja. Proses identifikasi ini tidak hanya berupa pernyataan hasil, tetapi didukung oleh bukti empiris dari hasil wawancara dengan 11 responden yang menyatakan bahwa gangguan yang sering terjadi pada sistem e-Kinerja meliputi downtime, kesalahan input data, dan potensi gangguan keamanan.

Berdasarkan transkrip wawancara, salah satu responden menyatakan:

“Dalam penggunaan e-Kinerja sering terjadi gangguan akses terutama pada jam sibuk yang menyebabkan sistem menjadi lambat” (Responden 2, Wawancara, Transkrip W1, Lampiran A).

Responden lain juga menyatakan:

“Kesalahan input data sering terjadi karena kurang teliti dalam pengisian laporan kinerja harian” (Responden 5, Wawancara, Transkrip W2, Lampiran A).

Selain itu:

“Pernah terjadi downtime sistem yang membuat layanan tidak dapat diakses sementara waktu” (Responden 8, Wawancara, Transkrip W3, Lampiran A).

Berdasarkan hasil wawancara, dapat dinilai bahwa terdapat beberapa jenis risiko yang terjadi pada sistem e-Kinerja, yaitu gangguan akses sistem pada jam sibuk yang menyebabkan keterlambatan layanan, kesalahan input data akibat faktor human error, serta kejadian downtime yang menyebabkan sistem tidak dapat diakses sementara waktu. Hal ini menunjukkan bahwa risiko operasional

pada sistem e-Kinerja benar-benar terjadi dan berdampak langsung terhadap kelancaran layanan. Dengan demikian, proses identifikasi risiko sudah berjalan berdasarkan pengalaman nyata pengguna, bukan hanya asumsi, sehingga menjadi dasar yang valid dalam pengelolaan risiko pada sistem e-Kinerja.

Proses identifikasi risiko dilakukan dengan tahapan pengumpulan data melalui wawancara dengan pengguna dan pengelola sistem untuk mengetahui pengalaman gangguan yang terjadi. Selanjutnya dilakukan observasi langsung terhadap penggunaan sistem e-Kinerja guna melihat kondisi nyata di lapangan. Selain itu, dilakukan analisis terhadap potensi gangguan berdasarkan data yang diperoleh, kemudian risiko-risiko yang teridentifikasi seperti gangguan akses, kesalahan input, dan downtime dicatat dan dikelompokkan sebagai daftar risiko. Hasil identifikasi ini selanjutnya menjadi dasar dalam tahap analisis risiko berikutnya.

Selain itu, hasil observasi terhadap penggunaan sistem menunjukkan adanya beberapa kendala operasional seperti keterlambatan akses sistem pada jam sibuk serta potensi error pada saat input data. Bukti lain juga diperkuat melalui dokumen pendukung dan catatan insiden yang menunjukkan adanya riwayat gangguan sistem yang menjadi dasar dalam proses identifikasi risiko. Dengan demikian, proses identifikasi risiko tidak hanya berdasarkan asumsi, tetapi berdasarkan data wawancara, observasi langsung, serta catatan kejadian pada sistem e-Kinerja.

3. Hasil evaluasi menunjukkan bahwa analisis risiko kualitatif dilakukan dengan menggunakan matriks risiko berdasarkan tingkat kemungkinan

(probability) dan dampak (impact) untuk menentukan tingkat prioritas risiko. Penentuan tingkat probability diperoleh dari hasil wawancara dengan responden terkait frekuensi terjadinya risiko, sedangkan dampak dinilai berdasarkan tingkat pengaruhnya terhadap layanan e-Kinerja.

Berdasarkan transkrip wawancara, salah satu responden menyatakan:

“Penilaian risiko biasanya dilihat dari seberapa sering gangguan terjadi dan seberapa besar dampaknya terhadap layanan e-Kinerja” (Responden 3, Wawancara, Transkrip W6, Lampiran A).

Responden lain juga menyatakan:

“Risiko yang sering terjadi seperti keterlambatan akses dinilai lebih tinggi prioritasnya karena sangat mengganggu pekerjaan pegawai” (Responden 6, Wawancara, Transkrip W7, Lampiran A).

Berdasarkan hasil wawancara, dapat dinilai bahwa analisis risiko kualitatif pada sistem e-Kinerja telah dilakukan dengan mempertimbangkan dua parameter utama, yaitu tingkat kemungkinan (probability) dan tingkat dampak (impact) dari suatu risiko. Risiko yang sering terjadi dan memiliki dampak besar terhadap layanan, seperti keterlambatan akses sistem, dinilai memiliki prioritas yang lebih tinggi dalam penanganannya. Hal ini menunjukkan bahwa proses penilaian risiko sudah menggunakan pendekatan berbasis tingkat urgensi, sehingga dapat membantu dalam menentukan prioritas penanganan risiko secara lebih tepat.

Proses analisis risiko kualitatif dilakukan dengan tahapan penentuan tingkat kemungkinan (probability) berdasarkan frekuensi terjadinya risiko yang diperoleh dari hasil wawancara. Selanjutnya, ditentukan tingkat dampak (impact) berdasarkan pengaruh risiko terhadap layanan e-Kinerja. Setelah itu, kedua parameter tersebut dipetakan ke dalam matriks risiko untuk menentukan tingkat prioritas masing-masing risiko (rendah, sedang, tinggi). Hasil dari pemetaan ini kemudian digunakan untuk menetapkan urutan prioritas penanganan risiko sesuai tingkat urgensinya.

4. Hasil evaluasi menunjukkan bahwa analisis risiko kuantitatif (sederhana) dilakukan dengan memperkirakan tingkat dampak risiko secara lebih terukur, seperti tingkat gangguan layanan atau potensi kerugian akibat terjadinya risiko.

Berdasarkan transkrip wawancara, salah satu responden menyatakan:

“Jika sistem e-Kinerja mengalami gangguan, maka pekerjaan pegawai bisa tertunda dan membutuhkan waktu tambahan untuk menyelesaikan laporan” (Responden 7, Wawancara, Transkrip W8, Lampiran A).

Responden lain juga menyatakan:

“Kerugian yang dirasakan lebih ke waktu kerja yang terbuang karena sistem tidak bisa diakses atau lambat” (Responden 9, Wawancara, Transkrip W9, Lampiran A).

Berdasarkan hasil wawancara, dapat dinilai bahwa dampak risiko pada

sistem e-Kinerja dapat diukur secara sederhana melalui gangguan terhadap waktu kerja dan keterlambatan penyelesaian tugas. Gangguan sistem seperti keterlambatan akses atau sistem tidak dapat digunakan menyebabkan pekerjaan pegawai tertunda dan membutuhkan waktu tambahan untuk menyelesaikan laporan. Hal ini menunjukkan bahwa risiko tidak hanya berdampak pada sistem, tetapi juga langsung mempengaruhi efisiensi kerja pegawai, terutama dari sisi kehilangan waktu kerja akibat gangguan layanan.

Proses analisis risiko kuantitatif (sederhana) dilakukan dengan

tahapan mengidentifikasi dampak risiko yang dapat diukur, seperti keterlambatan pekerjaan dan gangguan layanan. Selanjutnya, dilakukan estimasi besarnya dampak berdasarkan waktu yang terbuang atau frekuensi gangguan yang terjadi. Setelah itu, hasil pengukuran sederhana tersebut digunakan untuk menggambarkan tingkat kerugian atau dampak yang ditimbulkan oleh risiko. Hasil analisis ini kemudian digunakan untuk memperkuat penilaian dalam menentukan prioritas penanganan risiko.

5. Hasil evaluasi menunjukkan bahwa perencanaan respon risiko dilakukan dengan menentukan strategi penanganan terhadap setiap risiko yang telah dianalisis, seperti menghindari (avoid), mengurangi (mitigate), mentransfer (transfer), atau menerima (accept) risiko, serta menetapkan langkah-langkah yang akan diambil untuk menangani risiko tersebut.

Berdasarkan transkrip wawancara, salah satu responden menyatakan:

“Jika terjadi gangguan sistem, biasanya kami langsung mengurangi

dampaknya dengan melakukan perbaikan cepat atau melaporkan ke tim teknis” (Responden 3, Wawancara, Transkrip W10, Lampiran A).

Responden lain juga menyatakan:

“Untuk risiko tertentu seperti error ringan, biasanya dibiarkan dulu sambil dipantau, tapi kalau parah langsung ditangani oleh tim IT” (Responden 6, Wawancara, Transkrip W11, Lampiran A).

Berdasarkan hasil wawancara, dapat dinilai bahwa perencanaan respon risiko pada sistem e-Kinerja dilakukan secara fleksibel sesuai tingkat keparahan risiko yang terjadi. Risiko dengan dampak ringan ditangani dengan pemantauan terlebih dahulu, sedangkan risiko yang berdampak besar langsung dilakukan penanganan oleh tim teknis atau tim IT. Selain itu, langkah pengurangan dampak juga dilakukan melalui perbaikan cepat atau pelaporan langsung agar gangguan tidak berkepanjangan. Hal ini menunjukkan bahwa strategi respon risiko sudah diterapkan, meskipun masih bersifat reaktif sesuai kondisi yang terjadi.

Proses perencanaan respon risiko dilakukan dengan tahapan mengkaji hasil analisis risiko untuk menentukan tingkat keparahan masing-masing risiko. Selanjutnya, dipilih strategi penanganan yang sesuai, seperti mengurangi dampak melalui perbaikan cepat, melakukan pelaporan kepada tim teknis, atau melakukan pemantauan terhadap risiko dengan dampak ringan. Setelah itu, ditetapkan langkah-langkah penanganan yang akan dilakukan sesuai kondisi yang terjadi. Hasil dari proses ini kemudian digunakan sebagai acuan dalam menangani risiko secara langsung ketika gangguan terjadi.

6. Hasil evaluasi menunjukkan bahwa mitigasi risiko dilakukan melalui penerapan kontrol teknis dan administratif, seperti backup data, pengamanan sistem, dan pembatasan akses pengguna.

Berdasarkan transkrip wawancara, salah satu responden menyatakan:

“Data sistem e-Kinerja secara rutin dilakukan backup untuk mengantisipasi kehilangan data jika terjadi gangguan” (Responden 2, Wawancara, Transkrip W12, Lampiran A).

Responden lain juga menyatakan:

“Akses sistem dibatasi hanya untuk pegawai tertentu agar keamanan data tetap terjaga” (Responden 5, Wawancara, Transkrip W13, Lampiran A).

Berdasarkan hasil wawancara, dapat dinilai bahwa mitigasi risiko pada sistem e-Kinerja telah dilakukan melalui penerapan kontrol teknis dan administratif. Kontrol teknis dilakukan dengan melakukan backup data secara rutin untuk mengantisipasi kehilangan data ketika terjadi gangguan sistem. Sementara itu, kontrol administratif dilakukan dengan pembatasan akses sistem hanya kepada pegawai tertentu guna menjaga keamanan data. Hal ini menunjukkan bahwa upaya mitigasi risiko sudah diterapkan untuk mengurangi dampak dan mencegah terjadinya gangguan yang lebih besar pada sistem e-Kinerja.

Proses mitigasi risiko dilakukan dengan tahapan menentukan

tindakan pengendalian berdasarkan jenis risiko yang telah diidentifikasi. Selanjutnya, diterapkan kontrol teknis seperti backup data secara rutin untuk mencegah kehilangan data akibat gangguan sistem. Selain itu, diterapkan kontrol administratif berupa pembatasan akses pengguna untuk menjaga keamanan data. Setelah itu, dilakukan penerapan dan pengawasan terhadap kontrol yang telah ditetapkan guna memastikan mitigasi berjalan efektif dalam mengurangi dampak risiko.

7. Hasil evaluasi menunjukkan bahwa monitoring dan evaluasi risiko dilakukan melalui pemantauan berkala, evaluasi insiden, serta peninjauan ulang efektivitas mitigasi yang telah diterapkan.

Berdasarkan transkrip wawancara, salah satu responden menyatakan:

“Setiap ada gangguan sistem, selalu dicatat dan dievaluasi untuk mengetahui penyebabnya serta cara pencegahannya ke depan” (Responden 4, Wawancara, Transkrip W14, Lampiran A).

Responden lain juga menyatakan:

“Pemantauan sistem dilakukan secara berkala oleh tim IT untuk memastikan layanan e-Kinerja tetap berjalan dengan baik” (Responden 7, Wawancara, Transkrip W15, Lampiran A).

Berdasarkan hasil wawancara, dapat dinilai bahwa monitoring dan evaluasi risiko pada sistem e-Kinerja telah dilakukan secara berkelanjutan melalui pemantauan berkala oleh tim IT untuk memastikan sistem tetap berjalan

dengan baik. Selain itu, setiap kejadian gangguan juga dicatat dan dievaluasi untuk mengetahui penyebabnya serta sebagai dasar perbaikan dan pencegahan di masa mendatang. Hal ini menunjukkan bahwa proses monitoring dan evaluasi sudah berjalan dan berfungsi sebagai mekanisme umpan balik dalam pengelolaan risiko sistem e-Kinerja.

Proses monitoring dan evaluasi risiko dilakukan dengan tahapan melakukan pemantauan sistem secara berkala oleh tim IT untuk memastikan layanan berjalan dengan baik. Selanjutnya, setiap kejadian gangguan dicatat sebagai insiden dan dilakukan evaluasi untuk mengetahui penyebab serta dampaknya. Setelah itu, dilakukan peninjauan ulang terhadap efektivitas mitigasi yang telah diterapkan. Hasil evaluasi ini kemudian digunakan sebagai dasar perbaikan dan pencegahan risiko di masa mendatang, sehingga mendukung peningkatan pengelolaan risiko secara berkelanjutan.

Secara keseluruhan, ketujuh proses manajemen risiko telah dijalankan. Namun, tingkat kapabilitasnya masih bervariasi, di mana beberapa proses telah berjalan secara sistematis, tetapi belum sepenuhnya terdokumentasi dan terstandarisasi secara formal. Hal ini menunjukkan bahwa kapabilitas manajemen risiko berada pada tingkat Managed hingga Established.

Berdasarkan tujuh proses manajemen risiko tahapan ini menunjukkan bahwa proses manajemen risiko telah berjalan secara sistematis dan mencakup seluruh siklus manajemen risiko. Namun, implementasinya masih belum sepenuhnya terdokumentasi secara formal dan terintegrasi dalam satu kerangka manajemen risiko organisasi.

4.2 Hasil Pengolahan Data Kuisisioner COBIT 2019

Penentuan total akumulasi dari skala Likert dilakukan berdasarkan hasil pengisian kuisisioner yang terlibat langsung dalam tata kelola SPBE yaitu pengelolaan sistem e-Kinerja. Setiap pernyataan dinilai menggunakan skala Likert 1–5, kemudian dihitung nilai rata-rata setiap item dan dirata-ratakan kembali pada tingkat domain. Nilai rata-rata domain dipetakan ke *Capability Level* COBIT 2019 untuk mengetahui tingkat kapabilitas pengelolaan sistem e-Kinerja. pada Dinas Kominfo Kabupaten Blitar. Berikut hasil lengkap pengolahan data untuk masing-masing domain.

4.2.1 Domain EDM03 – Ensure Risk Optimization

Dari hasil kuisisioner dan wawancara yang telah dilakukan, diketahui bahwa pimpinan Dinas Komunikasi dan Informatika Kabupaten Blitar telah melakukan pengawasan dan pengendalian terhadap risiko pada sistem e-Kinerja. Pengendalian tersebut dilakukan melalui pemantauan ketersediaan layanan, tingkat keluhan pengguna, serta stabilitas sistem yang berjalan. Meskipun demikian, hasil temuan juga menunjukkan bahwa belum terdapat kebijakan formal yang secara spesifik mengatur batas toleransi risiko dalam bentuk bukti.

Berdasarkan hasil rekapitulasi kuisisioner, domain EDM03 memperoleh skor rata-rata 2,80 yang masuk kategori **Level 3: Established**. Domain ini menilai sejauh mana pimpinan membuat aturan, menentukan batas aman gangguan, dan mengawasi risiko agar tidak mengganggu kinerja ASN.

Rincian nilai per item EDM03

Tabel 4. 1 Hasil Penilaian Kapabilitas Domain EDM03 (Ensure Risk Optimization)

Item	Rata-rata	Level
Item 1 – Penetapan toleransi risiko	2,00	Level 2
Item 2 – Tinjauan efektivitas pengelolaan risiko	3,00	Level 3
Item 3 – Pemahaman pimpinan terhadap dampak risiko	4,00	Level 4
Item 4 – Keputusan berbasis analisis risiko	2,00	Level 2
Item 5 – Evaluasi berkala terhadap risiko utama	3,00	Level 3

Angka rata-rata pada Tabel 4.1 berasal dari hasil penilaian peneliti terhadap jawaban wawancara responden terkait penerapan proses manajemen risiko pada domain EDM03. Penilaian dilakukan dengan melihat sejauh mana praktik yang dijelaskan responden telah berjalan sesuai indikator COBIT 2019, seperti tingkat pelaksanaan, konsistensi, keterlibatan pimpinan, evaluasi risiko, dan formalitas proses yang dilakukan. Setelah jawaban wawancara dianalisis, peneliti memberikan nilai skala 1–5 pada setiap item berdasarkan tingkat kapabilitas yang terlihat dari hasil wawancara tersebut. Nilai-nilai tersebut kemudian dihitung sehingga menghasilkan angka rata-rata pada masing-masing item domain EDM03.

Interpretasi

Berdasarkan hasil penilaian pada Tabel 4.1, domain EDM03 menunjukkan tata kelola optimasi risiko telah terlembaga secara formal melalui pengawasan pimpinan yang aktif, namun belum sepenuhnya menjadi dasar dalam pengambilan keputusan strategis.

1. **Kekuatan Pengawasan (Level 4):** Skor tertinggi pada **pemahaman pimpinan terhadap dampak risiko (4,00)** menunjukkan bahwa jajaran

manajemen memiliki kesadaran tinggi dan pemahaman yang sangat baik terhadap risiko-risiko yang dapat mengganggu kinerja ASN.

2. **Kematangan Proses (Level 3):** Aspek **tinjauan efektivitas pengelolaan risiko** dan **evaluasi berkala terhadap risiko utama** telah berjalan secara konsisten dan terstandarisasi, memastikan adanya kontrol rutin terhadap potensi ancaman sistem e-Kinerja.
3. **Titik Lemah (Level 2):** Skor rendah pada **penetapan toleransi risiko (2,00)** dan **keputusan berbasis analisis risiko (2,00)** menunjukkan bahwa meskipun pimpinan memahami risiko, batasan risiko yang dapat diterima (*risk appetite*) belum diformalkan secara mendalam. Selain itu, hasil analisis risiko belum digunakan secara optimal sebagai rujukan utama dalam menentukan arah kebijakan atau pemilihan teknologi baru.

Jadi Tata kelola risiko pada domain EDM03 sudah melampaui tahap pengelolaan dasar karena adanya keterlibatan pimpinan yang rutin. Namun, instansi masih perlu memperkuat formalitas penetapan ambang batas risiko agar setiap keputusan strategis dapat diambil berdasarkan data profil risiko yang lebih akurat.

4.2.2 Domain APO12 – Manage Risk

Dari hasil kuisioner dan wawancara, proses manajemen risiko pada sistem e-Kinerja telah dilaksanakan melalui tahapan identifikasi, analisis, dan mitigasi risiko yang dilakukan secara operasional. Identifikasi risiko dilakukan melalui pemantauan sistem, bukti, serta analisis terhadap potensi ancaman yang mungkin terjadi. Namun demikian, hasil penelitian menunjukkan bahwa proses tersebut

belum sepenuhnya didukung oleh dokumentasi formal seperti standar prosedur pengelolaan risiko yang terdokumentasi dengan baik.

APO12 mendapatkan skor rata-rata 2,29 yang dipetakan pada **Level 2: Managed**. Domain ini menilai bagaimana staf bekerja mengidentifikasi ancaman, menganalisis dampak, dan mendokumentasikan e-Kinerja.

Rincian nilai per item APO12

Tabel 4. 2 Hasil Penilaian Kapabilitas Domain APO12 (Manage Risk)

Item	Rata-rata	Level
Item 1 – Identifikasi risiko	3,00	Level 3
Item 2 – Analisis risiko berdasarkan dampak & kemungkinan	3,00	Level 3
Item 3 – Tersedia rencana mitigasi untuk setiap risiko signifikan yang teridentifikasi.	3,00	Level 3
Item 4 – Setiap unit kerja memiliki tanggung jawab dalam pelaporan risiko.	3,00	Level 3
Item 5 – Pengendalian risiko telah terintegrasi dengan kebijakan keamanan informasi.	2,00	Level 2
Item 6 – Efektivitas mitigasi risiko dievaluasi berkala.	1,00	Level 1
Item 7 – Analisis risiko digunakan untuk perencanaan dan pengembangan sistem.	1,00	Level 1

Angka rata-rata pada Tabel 4.2 berasal dari hasil penilaian peneliti terhadap jawaban wawancara responden terkait penerapan manajemen risiko pada domain APO12. Penilaian dilakukan berdasarkan indikator COBIT 2019, seperti identifikasi risiko, analisis risiko, mitigasi risiko, pengendalian risiko, dan evaluasi risiko. Dari hasil wawancara tersebut, peneliti memberikan nilai skala 1–5 sesuai tingkat penerapan proses yang ditemukan, kemudian dihitung hingga menghasilkan angka rata-rata pada setiap item.

Interpretasi

Berdasarkan Tabel 4.2, domain APO12 menunjukkan proses manajemen risiko e-Kinerja telah dilaksanakan secara terencana dan terpantau, namun belum memberikan dampak strategis bagi organisasi.

1. **Kekuatan Operasional (Level 3):** Instansi sudah mampu melakukan **identifikasi, analisis, dan perencanaan mitigasi risiko** secara konsisten. Tanggung jawab pelaporan risiko juga telah terbagi dengan baik di setiap unit kerja.
2. **Kematangan Prosedur (Level 2):** Aspek **integrasi kebijakan keamanan informasi (2,00)** masih berada pada tahap pengelolaan dasar, di mana penyelarasan antara manajemen risiko dengan aturan keamanan formal belum sepenuhnya solid.

Titik Lemah (Level 1): Skor terendah pada **evaluasi mitigasi berkala (1,00)** dan **pemanfaatan analisis risiko untuk pengembangan sistem (1,00)** menunjukkan bahwa manajemen risiko saat ini baru sebatas pemenuhan administratif. Hasil analisis risiko belum digunakan sebagai landasan dalam perencanaan teknologi masa depan maupun perbaikan berkelanjutan.

Jadi Manajemen risiko sudah berjalan secara teknis, namun efektivitasnya masih bersifat reaktif karena minimnya evaluasi berkala dan belum dijadikannya profil risiko sebagai acuan utama dalam pengambilan keputusan pengembangan sistem. Meskipun telah mencapai

Level 3 (Established), hasil identifikasi risiko menunjukkan bahwa sebagian risiko krusial seperti keamanan data dan downtime telah teridentifikasi, sehingga kemampuan organisasi dalam mengenali risiko utama sudah cukup baik, meskipun masih perlu penyempurnaan pada aspek dokumentasi dan standarisasi.

Analisis risiko dilakukan menggunakan pendekatan matriks dampak dan kemungkinan. Setiap risiko dinilai berdasarkan tingkat dampaknya terhadap layanan e-Kinerja serta kemungkinan terjadinya.

- a. Risiko downtime sistem memiliki dampak tinggi dan kemungkinan sedang
- b. Risiko kebocoran data memiliki dampak sangat tinggi namun kemungkinan rendah
- c. Risiko kesalahan input data memiliki dampak sedang dengan kemungkinan tinggi

Hasil analisis ini digunakan untuk menentukan prioritas penanganan risiko.

4.2.3 Domain DSS04 – Manage Continuity

Dari hasil kuisioner dan wawancara, upaya menjaga keberlanjutan layanan sistem e-Kinerja telah dilakukan melalui penerapan mekanisme teknis seperti adanya bukti, serta pengelolaan infrastruktur yang mendukung ketersediaan layanan. Meskipun demikian, secara administratif belum terdapat dokumen formal seperti Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) yang secara khusus mengatur prosedur penanganan gangguan atau bencana secara

terstruktur dan terstandarisasi.

DSS04 memperoleh skor rata-rata 3,40 yang masuk kategori Level 3: Established. Domain ini menilai seberapa lama layanan e-Kinerja sanggup bertahan atau seberapa cepat bisa bangkit kembali jika terjadi bencana.

Tabel 4. 3 Hasil Penilaian Kapabilitas Domain DSS04 (Manage Continuity)

Item	Rata-rata	Level
Item 1 – Instansi memiliki rencana keberlanjutan layanan.	2,00	Level 2
Item 2 – Prosedur backup & recovery	3,00	Level 3
Item 3 – Uji pemulihan sistem	4,00	Level 4
Item 4 – Mekanisme tanggap darurat	4,00	Level 4
Item 5 – Evaluasi insiden untuk perbaikan	4,00	Level 4

Angka rata-rata pada Tabel 4.3 berasal dari hasil penilaian peneliti terhadap jawaban wawancara responden terkait penerapan keberlanjutan layanan pada domain DSS04. Penilaian dilakukan berdasarkan indikator COBIT 2019, seperti rencana keberlanjutan layanan, prosedur backup dan recovery, uji pemulihan sistem, mekanisme tanggap darurat, serta evaluasi insiden. Dari hasil wawancara tersebut, peneliti memberikan nilai skala 1–5 sesuai tingkat penerapan proses yang ditemukan, kemudian dihitung sehingga menghasilkan angka rata-rata pada setiap item.

Interpretasi

Berdasarkan hasil penilaian pada Tabel 4.3, menunjukkan bahwa mekanisme pemulihan dan tanggap darurat telah terstandarisasi serta berjalan secara prediktabel, namun keberlanjutan layanan secara keseluruhan masih terhambat oleh perencanaan strategis yang belum matang. Berikut adalah rincian interpretasinya:

1. **Kekuatan Operasional (Level 4):** Instansi sangat kuat dalam aspek teknis dan evaluasi, di mana **uji pemulihan sistem, mekanisme tanggap darurat, dan evaluasi insiden** sudah dilakukan secara konsisten dan terukur.
2. **Kematangan Prosedur (Level 3):** Aspek **backup & recovery** telah mengikuti standar prosedur yang baku dan dijalankan secara rutin.
3. **Titik Lemah (Level 2):** Skor terendah pada **rencana keberlanjutan layanan (2,00)** menunjukkan bahwa meskipun tindakan teknis saat terjadi gangguan sangat baik, instansi belum memiliki dokumen perencanaan jangka panjang yang terintegrasi secara menyeluruh di tingkat organisasi.

Jadi Secara teknis layanan e-Kinerja sangat resilien dan cepat bangkit dari gangguan, namun secara administratif masih memerlukan penguatan pada formalitas dokumen rencana keberlanjutan

Berdasarkan hasil analisis risiko yang telah dilakukan menggunakan pendekatan matriks dampak dan kemungkinan, dilakukan perencanaan mitigasi untuk mengurangi tingkat dampak dan kemungkinan terjadinya risiko pada layanan e-Kinerja. Proses ini merupakan bagian dari tahapan **risk response** dalam manajemen risiko.

Beberapa strategi mitigasi yang diterapkan antara lain:

1. Backup data secara berkala untuk mengantisipasi kehilangan data
2. Penerapan kontrol akses untuk mencegah kebocoran data
3. Pengujian sistem secara rutin untuk mengurangi risiko downtime

4. Pelatihan keamanan informasi bagi ASN
5. Penerapan firewall dan sistem keamanan jaringan

Implementasi mitigasi tersebut dilakukan secara berkelanjutan dan menjadi bagian dari aktivitas operasional layanan e-Kinerja. Selain itu, efektivitas mitigasi dievaluasi melalui proses audit, monitoring sistem, serta peninjauan ulang terhadap insiden yang terjadi. Hal ini menunjukkan bahwa proses mitigasi tidak hanya direncanakan, tetapi juga diimplementasikan dan diawasi secara berkesinambungan sesuai dengan prinsip manajemen risiko dalam COBIT 2019.

Berdasarkan hasil kuisioner dan wawancara, dapat diketahui bahwa pengelolaan risiko pada sistem e-Kinerja telah berjalan secara operasional, namun masih terdapat beberapa kekurangan dalam aspek tata kelola dan dokumentasi formal.

4.3 Hasil Analisis Kualitatif (Wawancara 11 Responden)

Analisis kualitatif dilakukan dengan menelaah seluruh jawaban wawancara dari 11 responden yang terlibat dalam pengelolaan layanan e-Kinerja. Temuan ini berfungsi untuk memperkuat hasil kuisioner dan menjelaskan alasan mengapa skor tiap domain berada pada level tertentu. Hasil wawancara memperlihatkan ukuran sistem e-Kinerja dalam bekerja.

Dari hasil analisis yang dilakukan, masih terdapat beberapa kesenjangan dalam penerapan manajemen risiko pada sistem e-Kinerja di Dinas Komunikasi dan Informatika Kabupaten Blitar. Kesenjangan tersebut meliputi belum adanya dokumen formal terkait penetapan batas toleransi risiko, belum dilaksanakannya

audit risiko secara rutin dan terjadwal. Kondisi ini menunjukkan bahwa penerapan manajemen risiko masih bersifat operasional dan belum sepenuhnya matang dalam aspek tata kelola.

4.3.1 Tema Utama dari Wawancara

Berdasarkan pengelompokan jawaban responden, muncul beberapa tema dominan berikut:

1. Tersedianya Kebijakan Formal dan Toleransi Risiko TI

Seluruh responden dari domain EDM03 menegaskan bahwa instansi sudah memiliki kebijakan tertulis terkait toleransi risiko TI, termasuk batas risiko yang dapat diterima. Keberadaan SOP, serta menjadi dasar konsistensi dalam pengambilan keputusan risiko.

2. Evaluasi Risiko Dilakukan Secara Berkala

Mayoritas responden menyampaikan bahwa pimpinan rutin melakukan Rapat Tinjauan Manajemen (RTM), evaluasi risiko e-Kinerja, dan peninjauan dokumen yang ada. Frekuensi RTM dilakukan minimal satu kali setahun, meskipun beberapa responden menilai cakupannya masih dapat diperluas.

3. Pelaksanaan dan Integrasi Risk Register

Semua responden menjelaskan bahwa Risk Register sudah ada, dikelola lintas bidang, dan memuat risiko teknis, risiko SDM, dan risiko operasional. Risk Register menjadi rujukan penting saat analisis risiko dan penyusunan mitigasi.

4. Identifikasi & Mitigasi Risiko Melibatkan Banyak Bidang

Responden dari APO12 menekankan bahwa proses identifikasi risiko berlangsung secara multidisiplin, melibatkan Koordinator Keamanan, Bidang

Kepegawaian, Tim Teknis Aplikasi, dan auditor internal. Mitigasi risiko dievaluasi melalui audit log, simulasi phishing, validasi kontrol akses, dan penegakan kebijakan.

5. Keberadaan DRP / BCP dan Kesiapan Insiden

Seluruh responden domain DSS04 menyatakan bahwa instansi memiliki dokumen BCP/DRP, dengan mekanisme backup harian, pengujian pemulihan berkala, serta target RTO-RPO yang jelas untuk e-Kinerja.

Koordinasi insiden dilakukan melalui Prosedur Manajemen Insiden (IRP) dan Protokol Komunikasi Insiden yang melibatkan Koordinator Manajemen Insiden, Tim Teknis, Keamanan SDM, dan pihak vendor.

6. Kendala Utama: Dokumentasi Mitigasi dan Sosialisasi

Dari ketiga domain, kendala terbesar yang muncul berulang adalah:

- a. Dokumentasi mitigasi yang belum seragam antar unit
- b. Sosialisasi BCP belum menjangkau seluruh ASN
- c. SDM teknis pemulihan sistem (DRC) masih terbatas
- d. Integrasi sistem lama dan baru masih menimbulkan risiko operasional

Tema-tema ini menjelaskan mengapa beberapa item tidak mencapai skor maksimal meskipun proses secara umum sudah berjalan baik.

4.3.2 Temuan per Domain

A. Domain EDM03 – Ensure Risk Optimization

Analisis wawancara menunjukkan bahwa tata kelola risiko SPBE dijalankan secara matang dan konsisten:

- a. **Pimpinan terlibat langsung dalam RTM**, peninjauan evaluasi risiko

utama, dan menetapkan kebijakan toleransi risiko formal.

- b. **Keputusan strategis menggunakan hasil analisis risiko**, termasuk pemilihan teknologi baru, kebijakan autentikasi, dan pengembangan fitur e-Kinerja. **Komunikasi risiko aktif** melalui laporan kepatuhan SDM (Sumber Daya Manusia), RTM (Rapat Tinjauan Manajemen), dan rapat SMKI (Sistem Manajemen Keamanan Informasi).

Seluruh temuan ini **konsisten dengan skor kuisisioner 2,80 (Level 3 – Established)**, menunjukkan bahwa tata kelola risiko telah terlembaga secara formal melalui keterlibatan aktif pimpinan dalam keputusan strategis dan komunikasi rutin, meskipun efektivitasnya masih perlu penguatan untuk mencapai efisiensi yang lebih tinggi.

B. Domain APO12 – Manage Risk

Jawaban responden memperlihatkan bahwa proses manajemen risiko berjalan terstruktur, namun masih terdapat variasi antar unit:

- a. Risiko e-Kinerja diidentifikasi secara menyeluruh mulai dari data, aplikasi, infrastruktur, hingga risiko SDM.
- b. Proses penilaian risiko menggunakan matriks dampak–kemungkinan, serta melibatkan Koordinator Keamanan, Tim Teknis Aplikasi, Kepegawaian, dan auditor internal. Berdasarkan hasil wawancara, penentuan tingkat kemungkinan (probability) dilakukan dengan melihat frekuensi kejadian risiko yang pernah terjadi pada sistem e-Kinerja, seperti seberapa sering gangguan sistem, kesalahan input, atau insiden keamanan muncul. Sementara itu, tingkat dampak (impact) dinilai

berdasarkan seberapa besar pengaruh risiko tersebut terhadap operasional layanan, seperti gangguan akses, kehilangan data, atau terganggunya aktivitas ASN. Beberapa responden menyatakan bahwa risiko seperti kesalahan input data termasuk sering terjadi (probability tinggi) namun berdampak sedang, sedangkan risiko kebocoran data jarang terjadi (probability rendah) tetapi memiliki dampak yang sangat tinggi terhadap organisasi.

- c. Mitigasi dilaksanakan dan dievaluasi melalui audit log, pelatihan keamanan, pemisahan tugas, simulasi phishing, dan review akses pegawai.
- d. Kendala utama yang ditemukan adalah ketidakkonsistenan dokumentasi mitigasi dan masih perlunya peningkatan koordinasi lintas bidang.

Temuan ini selaras dengan skor kuisioner **2,29 (Level 2 – *Managed*)**, menunjukkan bahwa manajemen risiko telah dikelola secara aktif melalui identifikasi dan mitigasi rutin, namun belum mencapai tahap standarisasi organisasi karena masih terdapat ketidakkonsistenan dokumentasi dan lemahnya koordinasi lintas bidang.

C. Domain DSS04 – *Manage Continuity*

Responden memberikan jawaban yang konsisten terkait kemampuan instansi menjaga keberlanjutan layanan:

- a. Seluruh responden menegaskan bahwa ada mekanisme tanggap darurat yang terstruktur, termasuk Post-Incident Review setelah gangguan.
- b. Koordinasi insiden berjalan melalui Tim Manajemen Insiden, dipimpin

Komandan Insiden dan melibatkan Koordinator Keamanan, BCM, Humas, vendor, dan unit kepegawaian.

- c. Tantangan utama meliputi kurangnya SDM teknis DRC bersertifikasi, integrasi sistem lama, dan keterbatasan anggaran untuk penguatan infrastruktur.
- d. Proses pemulihan dan komunikasi insiden dinilai cepat dan sudah mengikuti SOP yang ada.

Temuan ini menguatkan skor kuisisioner **3,40 (Level 3 – Established)** dan menunjukkan prosedur keberlangsungan layanan telah terstandarisasi secara formal, namun pengembangannya masih terhambat oleh keterbatasan SDM ahli dan anggaran infrastruktur pendukung.

Ringkasan Akhir Analisis Kualitatif

Keseluruhan hasil wawancara menunjukkan bahwa: **EDM03 berada pada level Established** karena proses pengawasan risiko sudah bukan lagi bersifat mendadak, melainkan sudah menjadi standar operasional yang baku di bawah kendali pimpinan.

- a. **APO12 berada pada level Managed**, karena identifikasi risiko sudah dijalankan, namun dokumentasi mitigasinya belum seragam dan koordinasi lintas bidang masih belum terstandarisasi secara menyeluruh.
- b. **DSS04 juga berada pada level Established**, namun pencapaiannya tertahan pada level ini akibat keterbatasan SDM teknis bersertifikasi dan belum optimalnya anggaran untuk memperkuat infrastruktur cadangan (*DRC*) secara menyeluruh.

Analisis kualitatif ini sepenuhnya sejalan dengan hasil kuisioner domain EDM03, APO12, dan DSS04, serta menggambarkan kondisi pengelolaan risiko SPBE pada layanan e-Kinerja di Dinas Kominfo Kabupaten Blitar.

4.4 Analisis Kapabilitas Menggunakan COBIT 2019

Analisis kapabilitas dilakukan dengan menggabungkan hasil kuisioner kuantitatif, temuan wawancara kualitatif, dan observasi pada proses pengelolaan risiko layanan e-Kinerja. Hasil ini menggambarkan kondisi kapabilitas proses SPBE pada layanan e-Kinerja di Dinas Kominfo secara menyeluruh.

Jadi , Penelitian ini menilai kemampuan Pemerintah Kabupaten Blitar dalam menjalankan seluruh proses manajemen risiko, mulai dari perencanaan, identifikasi, analisis kualitatif, analisis kuantitatif, mitigasi, implementasi, dan monitoring. Proses-proses tersebut menjadi bahan yang dinilai, sedangkan COBIT 2019 digunakan sebagai instrumen untuk mengukur tingkat kapabilitasnya.

4.4.1 Rekap Level Kapabilitas per Domain

Tabel berikut menyajikan nilai rata-rata setiap domain COBIT 2019 beserta level kapabilitasnya:

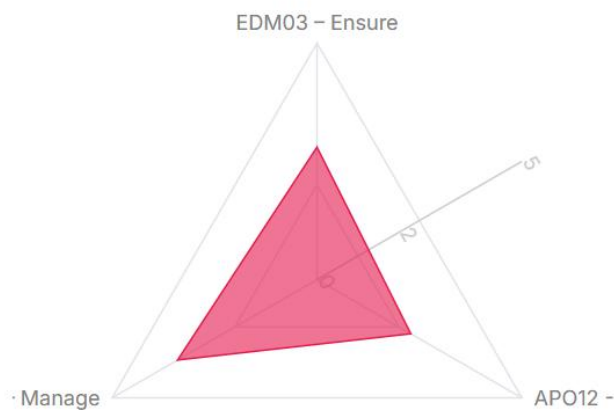
Tabel 4. 4 Rekapitulasi Nilai dan Level Kapabilitas Domain COBIT 2019

Domain	Rata-rata	Level COBIT 2019
EDM03 – <i>Ensure Risk Optimization</i>	2,80	Level 3 – <i>Established</i>
APO12 – <i>Manage Risk</i>	2,29	Level 2 – <i>Managed</i>
DSS04 – <i>Manage Continuity</i>	3,40	Level 3 – <i>Established</i>

Hasil rekap menunjukkan bahwa domain APO12 berada pada level terendah (*Managed*), sedangkan dua domain lainnya berada pada level *Established*,

Grafik Kematangan Domain

Visualisasi skor rata-rata gabungan per domain.



Gambar 4. 1 Grafik Kematangan Domain COBIT 2019 pada Layanan e-Kinerja

Gambar 4.1 menampilkan visualisasi tingkat kapabilitas manajemen risiko SPBE pada layanan e-Kinerja Dinas Komunikasi dan Informatika Kabupaten Blitar berdasarkan kerangka kerja COBIT 2019. Grafik tersebut menunjukkan skor rata-rata dari tiga domain yang dianalisis, yaitu EDM03 (Ensure Risk Optimization), APO12 (Manage Risk), dan DSS04 (Manage Continuity).

Domain APO12 memperoleh skor terendah dengan nilai 2,29 yang berada pada Level 2 (*Managed*), menunjukkan bahwa Manajemen risiko telah dilaksanakan secara terencana dan terpantau melalui penggunaan *Risk Register* dan matriks dampak, namun prosesnya belum terstandarisasi secara menyeluruh di

organisasi. Sementara itu, domain EDM03 dan DSS04 masing-masing memperoleh skor 2,80 dan 3,40 yang berada pada Level 3 (*Established*), yang menandakan bahwa pengawasan pimpinan (EDM03) serta mekanisme tanggap darurat (DSS04) bukan lagi sekadar upaya reaktif, melainkan sudah menjadi bagian dari budaya kerja organisasi yang didukung oleh SOP yang jelas.

Rumus Level Kematangan COBIT 2019

Skala penilaian yang digunakan untuk menentukan level.

Level 5 (Optimizing)	Skor: 4.50 - 5.00
Level 4 (Predictable)	Skor: 3.50 - 4.49
Level 3 (Established)	Skor: 2.50 - 3.49
Level 2 (Managed)	Skor: 1.50 - 2.49
Level 1 (Performed)	Skor: 0.50 - 1.49
Level 0 (Incomplete)	Skor: 0.00 - 0.49

Gambar 4. 2 Skala Penentuan Level Kapabilitas COBIT 2019

Gambar 4.2 menunjukkan skala penilaian yang digunakan untuk menentukan level kapabilitas proses berdasarkan COBIT 2019. Skala ini digunakan untuk memetakan nilai rata-rata hasil kuisioner ke dalam level kapabilitas, mulai dari Level 0 (*Incomplete*) hingga Level 5 (*Optimizing*).

4.4.2 Gap Analysis (Kondisi Existing vs Ideal)

Analisis gap dilakukan dengan membandingkan kondisi kondisi saat ini

dengan kondisi target menurut COBIT 2019, yaitu Level 3 – Established untuk seluruh domain manajemen risiko SPBE.

1. EDM03 – Ensure Risk Optimization

Existing: Level 3

Ideal: Level 5

Gap: 2 level

Tata kelola risiko sudah terstandarisasi secara formal dan pimpinan sudah terlibat. Namun, belum mencapai level optimal karena penetapan ambang batas risiko (*risk appetite*) belum diformalkan dan keputusan strategis belum sepenuhnya berbasis data risiko.

2. APO12 – Manage Risk

Existing: Level 2

Ideal: Level 5

Gap: 3 Level

Manajemen risiko sudah terencana, namun belum masuk kategori *Established* (Level 3) karena dokumentasi mitigasi masih tidak konsisten dan evaluasi berkala belum berjalan maksimal.

3. DSS04 – Manage Continuity

Existing: Level 3

Ideal: Level 5

Gap: 2 Level

Prosedur pemulihan layanan sudah kuat dan memiliki SOP baku. Namun, belum mencapai level *Predictable* (Level 4) atau *Optimizing*

(Level 5) karena kendala keterbatasan SDM teknis bersertifikasi dan infrastruktur pendukung yang belum maksimal.

4.4.3 Pembahasan

Pembahasan ini memadukan data kuisioner, hasil wawancara, dan observasi untuk menjelaskan penyebab setiap level kapabilitas.

A. EDM03 – Ensure Risk Optimization (Level 3 – Established)

Domain EDM03 mencapai Level 3 dengan skor 2,80, yang menunjukkan bahwa:

- a. Kekuatan: Pimpinan telah memiliki pemahaman yang sangat kuat mengenai dampak risiko (Skor 4,00) dan aktif melakukan tinjauan melalui Rapat Tinjauan Manajemen (RTM).
- b. Kelemahan: Capaian tertahan di Level 3 karena penetapan toleransi risiko dan pengambilan keputusan strategis berbasis risiko (Skor 2,00) belum sepenuhnya diformalkan. Instansi sudah memiliki budaya sadar risiko, namun belum tertuang dalam kebijakan tertulis yang rigid.

B. APO12 – Manage Risk (Level 2 – Managed)

Domain APO12 berada pada Level 2 dengan skor 2,29, menunjukkan bahwa:

- a. Kekuatan: Proses identifikasi dan penilaian risiko menggunakan matriks dampak-kemungkinan sudah dilakukan secara terencana oleh unit-unit kerja terkait.
- b. Kelemahan: Masih terdapat gap sejauh 3 level menuju kondisi ideal. Hal ini disebabkan oleh ketidakkonsistenan dokumentasi mitigasi antar unit serta belum berjalannya evaluasi berkala terhadap efektivitas mitigasi

(Skor 1,00).

Manajemen risiko saat ini masih bersifat administratif dan belum menjadi dasar dalam perencanaan pengembangan sistem di masa depan.

C. DSS04 – Manage Continuity (Level 3 – Established)

Domain DSS04 berada pada Level 3 dengan skor 3,40, menunjukkan bahwa:

- a. Kekuatan: Secara teknis, instansi sangat kuat dalam aspek uji pemulihan, mekanisme tanggap darurat, dan evaluasi insiden (Skor 4,00). Prosedur *backup* dan *recovery* juga telah berjalan sesuai standar.
- b. Kelemahan: Meskipun secara operasional sudah sangat baik, domain ini belum mencapai Level 4 atau 5 karena dokumen rencana keberlanjutan layanan (BCP) secara menyeluruh masih berada di level dasar (Skor 2,00). Selain itu, keterbatasan SDM teknis bersertifikasi dan anggaran infrastruktur menjadi hambatan utama dalam mencapai optimasi penuh.

Hasil penelitian ini juga didukung oleh dokumen SKP ASN yang menunjukkan adanya aktivitas pengelolaan risiko, seperti kegiatan backup data, pemeliharaan keamanan sistem, dan pelaporan kinerja. Aktivitas tersebut mencerminkan implementasi mitigasi risiko dan monitoring dalam manajemen risiko SPBE, khususnya pada layanan e-Kinerja. Namun, SKP belum secara eksplisit mencerminkan proses identifikasi dan analisis risiko secara sistematis.

Berdasarkan analisis dokumen SKP ASN, terdapat beberapa aktivitas yang dapat dikaitkan dengan proses manajemen risiko pada layanan e-Kinerja. Aktivitas seperti *backup data pada basis data*, *pemeliharaan dan keamanan sistem*, serta *pelaporan hasil pelaksanaan tugas* menunjukkan adanya

implementasi tahap mitigasi dan monitoring risiko. Kegiatan backup data berfungsi untuk mengurangi risiko kehilangan data, sedangkan pemeliharaan dan pengamanan sistem bertujuan untuk mencegah gangguan layanan maupun ancaman keamanan informasi.

Dari hasil analisis yang diperoleh dari kuisisioner dan wawancara, dapat disimpulkan bahwa Dinas Komunikasi dan Informatika Kabupaten Blitar telah menerapkan manajemen risiko pada sistem e-Kinerja. Namun, penerapan tersebut masih memerlukan penguatan pada aspek tata kelola, khususnya dalam penyusunan kebijakan formal, dokumentasi risiko, serta standarisasi prosedur agar sesuai dengan kerangka kerja COBIT 2019 secara menyeluruh.

Berikut penjelasan singkat:

- a. BCP** = *Business Continuity Plan*
- b.** (Rencana keberlangsungan layanan saat terjadi gangguan)
- c. DRP** = *Disaster Recovery Plan* (Rencana pemulihan sistem setelah bencana atau kerusakan)
- d. DRC** = *Disaster Recovery Center*
(Pusat/fasilitas pemulihan untuk menjalankan sistem saat terjadi gangguan)
- e. SDM teknis DRC** = Sumber Daya Manusia teknis yang bertugas mengelola dan mengoperasikan *Disaster Recovery Center*
- f. IRP** = *Incident Response Plan* (Rencana Tanggap Insiden)
- g. BCM** = *Business Continuity Management* (proses untuk memastikan layanan tetap berjalan saat terjadi gangguan atau bencana)

4.5 Integrasi Islam: *Mu'amalah ma'a Allah & Mu'amalah Ma'a an-nas*

Sebagai penelitian di lingkungan Universitas Islam Negeri (UIN), integrasi nilai-nilai Islam menjadi bagian penting dalam menganalisis implementasi manajemen risiko SPBE. Aktivitas pengelolaan risiko, pengamanan data, dan peningkatan keberlanjutan layanan e-Kinerja bukan hanya proses teknis, tetapi juga memiliki dimensi spiritual dan sosial yang selaras dengan prinsip mu'amalah dalam Islam, baik kepada Allah maupun kepada sesama manusia.

4.5.1 *Mu'amalah kepada Allah*

Penelitian ini memiliki hubungan langsung dengan nilai ketaatan kepada Allah SWT melalui prinsip kehati-hatian, profesionalitas, dan amanah dalam menjalankan tugas. Konsep manajemen risiko selaras dengan firman Allah dalam QS. An-Nisa' ayat 58:

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا وَإِذَا حَكَمْتُمْ بَيْنَ النَّاسِ أَنْ تَحْكُمُوا بِالْعَدْلِ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُمْ بِهِ ۚ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا ﴿٥٨﴾

“Sesungguhnya Allah menyuruh kamu menyampaikan amanah kepada pemiliknya. Apabila kamu menetapkan hukum di antara manusia, hendaklah kamu tetapkan secara adil. Sesungguhnya Allah memberi pengajaran yang paling baik kepadamu. Sesungguhnya Allah Maha Mendengar lagi Maha Melihat.” (QS. An-Nisa':58)

Ayat ini menegaskan bahwa setiap tanggung jawab harus dijalankan secara amanah dan profesional. Dalam penelitian ini, pengelolaan risiko sistem informasi merupakan bentuk menjaga amanah agar data dan layanan publik tetap aman dan berkelanjutan.

Menurut tafsir dalam *Tafsir Al-Misbah*, amanah mencakup seluruh

tanggung jawab yang berdampak pada orang lain (Kholifah, 2023). Dalam konteks modern, hal ini berarti menjaga keamanan data dan keberlangsungan layanan publik.

Sementara itu, dalam Tafsir *Ibnu Katsir* karya *Ibnu Katsir*, dijelaskan bahwa amanah mencakup seluruh kewajiban yang dipercayakan kepada manusia, baik dalam urusan agama maupun kehidupan sosial (Safrudin et al., 2023).

QS. Al-Mu'minun Ayat 8:

وَالَّذِينَ هُمْ لِأَمْتِهِمْ وَعَهْدِهِمْ رَاعُونَ ﴿٨﴾

“(Sungguh beruntung pula) orang-orang yang memelihara amanat dan janji mereka.” (QS. Al-Mu'minun: 8)

Menurut tafsir dalam *Tafsir Al-Misbah*, menjaga amanah merupakan ciri orang beriman dan mencakup tanggung jawab sosial serta profesional (Shihab, 2024). Dalam *Tafsir Ibnu Katsir* dijelaskan bahwa memelihara amanah berarti tidak mengkhianati kepercayaan, baik dalam urusan agama maupun dunia (Ibnu Katsir, 2025).

Dalam *Sahih Bukhari*, Rasulullah SAW bersabda:

إِذَا ضُبِعَتِ الْأَمَانَةُ فَانْتَظِرِ السَّاعَةَ

“Apabila amanah disia-siakan, maka tunggulah kehancuran.” (HR. Bukhari)

Maknanya: setiap tanggung jawab (termasuk pengelolaan sistem dan data) harus dijalankan secara profesional.

Jika dikaitkan dengan penelitian ini, maka pengelolaan risiko SPBE merupakan bentuk implementasi amanah dalam menjaga sistem digital agar tetap

aman, andal, dan berkelanjutan.

Artinya:

- a. Risiko kebocoran data = amanah yang harus dijaga
- b. Sistem layanan publik = tanggung jawab pemerintah
- c. Evaluasi risiko = bentuk profesionalitas kerja

Dengan demikian, manajemen risiko informasi dalam SPBE tidak hanya bernilai teknis, tetapi juga bernilai ibadah karena merupakan bagian dari menjalankan amanah.

Dalam konteks ini:

- a. Mitigasi risiko SPBE merupakan bentuk *ikhtiar* untuk menghindari bahaya dan menjaga keberlangsungan layanan.
- b. Menjaga keamanan data pegawai adalah bentuk menjaga amanah, karena data pribadi merupakan titipan yang harus dijaga integritas dan kerahasiaannya.
- c. Tindakan preventif dan pengawasan risiko mencerminkan ketakwaan melalui profesionalitas dan kehati-hatian dalam bekerja.

Maka, seluruh proses dalam penelitian ini, mulai dari identifikasi risiko, evaluasi risiko, hingga penyusunan rekomendasi, merupakan bagian dari mu'amalah kepada Allah, karena berorientasi pada amanah, kehati-hatian, dan pengabdian yang profesional.

4.5.2 Mu'amalah kepada Manusia (*Mu'amalah Ma'an-nas*)

Selain hubungan kepada Allah, Islam juga menekankan hubungan antar

manusia (*mu'amalah ma'an-nas*). Dalam konteks organisasi pemerintahan, kerja sama dalam mengelola risiko menjadi hal yang sangat penting.

Allah SWT berfirman dalam QS. Al-Ma'idah ayat 2:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَحْلُوا شَعَائِرَ اللَّهِ وَلَا الشَّهْرَ الْحَرَامَ وَلَا الْهَدْيَ وَلَا الْقَلَائِدَ وَلَا آمِينَ الْبَيْتِ الْحَرَامِ
يَبْتَغُونَ فَضْلًا مِّن رَّحْمَتِهِمْ وَرِضْوَانًا وَإِذَا حَلَلْتُمْ فَاصْطَادُوا وَلَا يَجْرِمَنَّكُمْ شَنَاٰنُ قَوْمٍ أَن صَدُّوكُمْ عَنِ
الْمَسْجِدِ الْحَرَامِ أَن تَعْتَدُوا وَتَعَاوَنُوا عَلَى الْبِرِّ وَالتَّقْوَىٰ وَلَا تَعَاوَنُوا عَلَى الْإِثْمِ وَالْعُدْوَانِ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ
شَدِيدُ الْعِقَابِ ﴿٢﴾

“Wahai orang-orang yang beriman, janganlah kamu melanggar syiar-syiar (kesucian) Allah, jangan (melanggar kehormatan) bulan-bulan haram, jangan (mengganggu) hadyu (hewan-hewan kurban) dan qalā'id (hewan-hewan kurban yang diberi tanda), dan jangan (pula mengganggu) para pengunjung Baitulharam sedangkan mereka mencari karunia dan rida Tuhannya! Apabila kamu telah bertahalul (menyelesaikan ihram), berburulah (jika mau). Janganlah sekali-kali kebencian(-mu) kepada suatu kaum, karena mereka menghalang-halangi kamu dari Masjidilharam, mendorongmu berbuat melampaui batas (kepada mereka). Tolong-menolonglah kamu dalam (mengerjakan) kebajikan dan takwa, dan jangan tolong-menolong dalam berbuat dosa dan permusuhan. Bertakwalah kepada Allah, sesungguhnya Allah sangat berat siksaan-Nya.(QS. Al-Ma'idah : 2)

Ayat ini menjelaskan pentingnya kolaborasi dalam kebaikan, termasuk dalam menjaga keamanan sistem informasi dan pelayanan publik.

Menurut tafsir *Al-Misbah*, ayat ini menekankan bahwa setiap aktivitas sosial harus diarahkan pada kemaslahatan bersama (Mufida, 2022). Dalam konteks organisasi, kerja sama antar unit menjadi faktor penting dalam mengurangi risiko.

Dalam tafsir *Ibnu Katsir*, dijelaskan bahwa manusia diperintahkan untuk saling membantu dalam hal yang membawa manfaat serta mencegah kerusakan (Hidayatallah et al., 2025). Sebagaimana ditegaskan dalam hadis riwayat Sahih Muslim, Rasulullah SAW bersabda:

وَاللَّهُ فِي عَوْنِ الْعَبْدِ مَا كَانَ الْعَبْدُ فِي عَوْنِ أَخِيهِ

“Allah akan menolong hamba-Nya selama hamba tersebut menolong saudaranya.” (HR. Muslim)

Hadis ini memperkuat perintah dalam QS. Al-Ma'idah: 2 tentang kewajiban saling membantu dalam kebaikan dan mencegah kerusakan.

QS. At-Taubah Ayat 71:

وَالْمُؤْمِنُونَ وَالْمُؤْمِنَاتُ بَعْضُهُمْ أَوْلِيَاءُ بَعْضٍ يَأْمُرُونَ بِالْمَعْرُوفِ وَيَنْهَوْنَ عَنِ الْمُنْكَرِ وَيُقِيمُونَ الصَّلَاةَ وَيُؤْتُونَ الزَّكَاةَ وَيُطِيعُونَ اللَّهَ وَرَسُولَهُ ۚ أُولَٰئِكَ سَيَرْحَمُهُمُ اللَّهُ إِنَّ اللَّهَ عَزِيزٌ حَكِيمٌ ﴿٧١﴾

“Orang-orang mukmin, laki-laki dan perempuan, sebagian mereka menjadi penolong bagi sebagian yang lain. Mereka menyuruh (berbuat) makruf dan mencegah (berbuat) mungkar, menegakkan salat, menunaikan zakat, dan taat kepada Allah dan Rasul-Nya. Mereka akan diberi rahmat oleh Allah. Sesungguhnya Allah Mahaperkasa lagi Mahabijaksana.” (QS.At-Taubah : 71)

Menurut tafsir dalam *Tafsir Al-Misbah*, ayat ini menjelaskan bahwa orang beriman saling menjadi penolong dalam kebaikan dan mencegah kemungkaran sebagai bentuk tanggung jawab sosial (Shihab, 2022).

Sementara itu, dalam *Tafsir Ibnu Katsir* dijelaskan bahwa kaum mukmin diperintahkan untuk saling membantu dalam ketaatan dan mencegah kerusakan (Ibnu Katsir, 2024).

Dalam *Sahih Muslim*, Rasulullah SAW bersabda:

وَاللَّهُ فِي عَوْنِ الْعَبْدِ مَا كَانَ الْعَبْدُ فِي عَوْنِ أَخِيهِ

“Allah akan menolong hamba-Nya selama hamba tersebut menolong saudaranya.” (HR. Muslim)

Maknanya: kerja sama dalam manajemen risiko dianjurkan dalam Islam. Al-Hujurat: 12

يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَحْسَسُوا وَلَا يَغْتَبَ بَعْضُكُم بَعْضًا ۚ الْحَبِيبُ

أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ ﴿١٢﴾

“Wahai orang-orang yang beriman, jauhilah banyak prasangka! Sesungguhnya sebagian prasangka itu dosa. Janganlah mencari-cari kesalahan orang lain dan janganlah ada di antara kamu yang menggunjing sebagian yang lain. Apakah ada di antara kamu yang suka memakan daging saudaranya yang sudah mati? Tentu kamu merasa jijik. Bertakwalah kepada Allah! Sesungguhnya Allah Maha Penerima Tobat lagi Maha Penyayang.” (QS. Al-Hujurat: 12)

Menurut tafsir Al-Misbah karya M. Quraish Shihab, ayat ini melarang mencari-

cari aib dan membuka rahasia orang lain karena dapat merusak kehormatan dan kepercayaan sosial (Shihab, 2023).

Dalam Tafsir *Ibnu Katsir*, dijelaskan bahwa larangan *tajassus* (mencari-cari kesalahan) mencakup membuka hal-hal yang seharusnya dijaga kerahasiaannya (Ibnu Katsir, 2024).

Dalam hadis riwayat Sahih Muslim, Rasulullah SAW bersabda:

لَا تَجَسَّسُوا وَلَا تَحَسَّسُوا

“Janganlah kalian saling memata-matai (*tajassus*) dan jangan saling mencari-cari kesalahan.” (HR. Muslim)

Hadis ini memperkuat larangan dalam QS. Al-Hujurat: 12 tentang kewajiban menjaga kehormatan dan kerahasiaan sesama manusia.

Jika dikaitkan dengan penelitian ini, maka:

- a. Pengelolaan risiko SPBE tidak bisa dilakukan sendiri
- b. Harus melibatkan tim TI, manajemen, dan pengguna sistem
- c. Tujuannya untuk melindungi masyarakat dari gangguan layanan

Hal ini menunjukkan bahwa manajemen risiko SPBE merupakan bentuk implementasi nilai tolong-menolong dalam menjaga kepentingan publik.

Integrasi *mu'amalah ma'annas* tercermin melalui:

- a. Perlindungan data pribadi ASN, yang merupakan hak setiap manusia dan harus dijaga dari penyalahgunaan.
- b. Peningkatan keamanan layanan publik, sehingga pelayanan tetap berjalan tanpa gangguan walaupun terjadi insiden teknis.
- c. Menjaga keberlangsungan layanan e-Kinerja, yang berdampak pada kelancaran administrasi kepegawaian seluruh ASN Kabupaten Blitar.
- d. Mencegah kerugian publik akibat kehilangan data, gangguan layanan, dan risiko keamanan.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian menggunakan kerangka kerja COBIT 2019, dapat disimpulkan bahwa kapabilitas manajemen risiko SPBE pada layanan e-Kinerja di Dinas Komunikasi dan Informatika Kabupaten Blitar berjalan dengan baik. **Domain APO12 berada pada Level 2 (*Managed*)**, yang menunjukkan manajemen risiko telah direncanakan, dipantau, namun prosesnya belum terstandarisasi secara konsisten di seluruh organisasi. **Sementara itu, domain EDM03 dan DSS04 berada pada Level 3 (*Established*)**, yang menandakan tata kelola dan keberlanjutan layanan telah memiliki prosedur yang terstandarisasi untuk dijalankan secara konsisten. Meskipun demikian, **masih diperlukan peningkatan pada aspek dokumentasi, koordinasi lintas unit, serta sosialisasi kebijakan** agar seluruh proses pengelolaan risiko SPBE dapat mencapai tingkat optimasi secara menyeluruh.

5.2 Saran

1. Dinas Komunikasi dan Informatika Kabupaten Blitar disarankan untuk meningkatkan standarisasi dan konsistensi dokumentasi manajemen risiko SPBE, khususnya pada layanan e-Kinerja.
2. Diperlukan peningkatan sosialisasi kebijakan keberlanjutan layanan dan manajemen risiko kepada seluruh ASN agar pemahaman dan kesiapan menghadapi risiko semakin merata.

3. Penelitian selanjutnya dapat memperluas cakupan domain COBIT 2019 atau menggunakan objek penelitian yang berbeda untuk memperoleh hasil yang lebih komprehensif.

DAFTAR PUSTAKA

- Amali, L. N., Katili, M. R., & Suhada, S. (2023). Core model of Information Technology Governance System Design in Local Government. *Telkomnika (Telecommunication Computing Electronics and Control)*, 21(4), 750. <https://doi.org/10.12928/telkomnika.v21i4.24287>
- Anugrah, R., Utami, E., & Muhammad, A. H. (2022). Analisis Manajemen Risiko TI Pada Perguruan Tinggi XYZ Berbasis COBIT 2019 dengan Pertimbangan Domain APO12. *Jurnal Ilmiah Universitas Batanghari Jambi*, 22(2), 991. <https://doi.org/10.33087/jiubj.v22i2.2175>
- Aryati, T., Khomsiyah, K., & Harahap, C. D. (2023). Enterprise risk management: A bibliometric analysis of research Trends. *Decision Science Letters*, 12(3), 561–570. <https://doi.org/10.5267/j.dsl.2023.4.007>
- Boniface Okanga. (2023). Local Government Project Risk Management Maturity Measurement model for Leveraging Effectiveness of Local Government Project Risk Management. *Journal of Management and Science*, 13(2), 62–69. <https://doi.org/10.26524/jms.13.23>
- Borysenko, V. D. (2023). Electronic government in public administration. *Uzhhorod National University Herald. Series: Law*, 2(76), 36–40. <https://doi.org/10.24144/2307-3322.2022.76.2.5>
- Cerqueira Junior, A. S., & Arima, C. H. (2023). Cyber Risk Management and ISO 27005 Applied In Organizations: A Systematic Literature Review. *Revista Foco*, 16(02), e1188. <https://doi.org/10.54751/revistafoco.v16n2-215>
- Chen, Y. (2023). The Past, Present, and Future of Enterprise Resource Planning. *Journal of Enterprise and Business Intelligence*, 65–74. <https://doi.org/10.53759/5181/JEBI202303007>
- Darmi, Y., Fernandez, S., Fathoni, M. Y., & Wijayanto, S. (2024). Evaluation of Governance in Information Systems Security to Minimize Information Technology Risks. *Intensif: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, 8(1), 40–51. <https://doi.org/10.29407/intensif.v8i1.21221>
- Fatayat, F. (2023). Analisis Tata Kelola Teknologi Informasi Perekaman E-KTP pada Dinas Kependudukan dan Pencatatan Sipil Kota Pekanbaru menggunakan Framework COBIT 2019. *Jurnal Minfo Polgan*, 12(1), 694–704. <https://doi.org/10.33395/jmp.v12i1.12492>
- Fianty, M. I., & Brian, M. (2023). Leveraging COBIT 2019 Framework to Implement IT Governance in Business Process Outsourcing Company.

Journal of Information Systems and Informatics, 5(2), 568–579.
<https://doi.org/10.51519/journalisi.v5i2.492>

- Haster, A. P., & Hartomo, K. D. (2022). Analisis tingkat kematangan Smart City Kabupaten Lombok Utara menggunakan COBIT 2019. *Jurnal Media Informatika Budidarma*, 6(3), 1459. <https://doi.org/10.30865/mib.v6i3.4344>
- Humaira, S., Nama, G. F., & Pradipta, R. A. (2024). Analisis Tata Kelola Teknologi Informasi menggunakan COBIT 2019 Subdomain DSS01 Manage Operations (Studi Kasus PT. BRI BO Liwa). *Jurnal Informatika dan Teknik Elektro Terapan*, 12(2).
<https://doi.org/10.23960/jitet.v12i2.4254>
- Haddad, H. (2023). Implementing risk management in local authorities: An exploratory case study of Moroccan municipalities. *International Journal of Public Policy and Administration Research*, 10(1), 34–45.
<https://doi.org/10.18488/74.v10i1.3320>
- Hidayatallah, F., Mahmudin Bunyamin, & Ahmad Muttaqin. (2025). Nilai Īsār dalam Perspektif Tafsir Tematik: Studi atas Ayat-Ayat Al-Qur'an tentang Solidaritas Sosial. *Al-Fahmu: Jurnal Ilmu Al-Qur'an dan Tafsir*, 4(2), 508–528. <https://doi.org/10.58363/alfahmu.v4i2.499>
- Kunio, N. I. H., Utami, E., & Muhammad, A. H. (2022). Audit Tata Kelola TI berbasis COBIT 2019 di Politeknik XYZ. *Jurnal Ilmiah Universitas Batanghari Jambi*, 22(2), 876. <https://doi.org/10.33087/jiubj.v22i2.1994>
- Kholifah, V. N. (2023). Konsep Keadilan dalam Al-Qur'an Studi Komparasi Tafsir Al-Misbah dan Tafsir Marah Labid terhadap Ayat-Ayat Adil. *Qaf: Jurnal Ilmu Al-Qur'an dan Tafsir*, 4(2), 127–159.
<https://doi.org/10.59579/qaf.v4i2.4181>
- Lompoliu, E., & William Tangka, G. M. (2024). Information Technology Governance Using the COBIT 2019 Framework at PT Bank Pembangunan Daerah Papua. *International Journal of Engineering, Science and Information Technology*, 4(4). <https://doi.org/10.52088/ijesty.v4i4.609>
- Lubna, L., Muhammad, A. H., & Purwanto, A. (2023). Identifikasi Level Tata Kelola TI dan Penilaian Tingkat Capability Level menggunakan COBIT 2019. *Jipi (jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 8(3), 815–827. <https://doi.org/10.29100/jipi.v8i3.3947>
- Mr. N. Suresh, Dr T. Varalakshmi, & Mohd Shoaib Chand. (2024). IT Governance Framework Ensuring Effective Management and Compliance. *International Research Journal on Advanced Engineering and Management (IRJAEM)*, 2(05), 1627–1632. -

<https://doi.org/10.47392/IRJAEM.2024.0227>

Mufida, M. H. (2022). Menelaah Al-Qur'an dan Hadist Filantropi Islam "Perbandingan Tafsir Ibnu Kastir dan Tafsir Fi Zhilalil Qur'an." *Al-Munir: Jurnal Studi Ilmu Al-Qur'an dan Tafsir*, 4(02), 299–334.
<https://doi.org/10.24239/al-munir.v4i2.136>

Nisa', F. Z., Febrianti, G. D., & Ajrina, N. N. (2023). Systematic Literature Review: Analisis Implementasi Manajemen Risiko TI Menggunakan Framework COBIT di Sektor Industri Jasa. *Bulletin of Computer Science Research*, 4(1), 66–74.
<https://doi.org/10.47065/bulletincsr.v4i1.313>

Safrudin, Moh., Nasaruddin, N., & Ihwan, I. (2023). "Tafsir Ayat-Ayat Kemasyarakatan" Implementasi Nilai-Nilai Kemanusiaan dalam Kehidupan Modern. *TAJDID: Jurnal Pemikiran Keislaman dan Kemanusiaan*, 7(1), 135–148. <https://doi.org/10.52266/tadjid.v7i1.1851>

Tanjung, D. F., Oktaviana, A., & Widodo, A. P. (2021). Analisis Manajemen Risiko Startup pada Masa Pandemi COVID-19 menggunakan COBIT® 2019. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 8(3), 635.
<https://doi.org/10.25126/jtiik.2021834914>

Taryoko, T., Muhammad, A. H., & Kusnawi, K. (2024). Analisis Rekomendasi untuk Meningkatkan Nilai Capability Level Domain APO 14 pada COBIT 2019. *Jurnal Ilmiah Universitas Batanghari Jambi*, 24(1), 888.
<https://doi.org/10.33087/jiubj.v24i1.4380>

Yohana, D. (2022). Audit Sistem Informasi Surat Menyurat pada Diskominfo Kota Bekasi dengan Kerangka Kerja COBIT 2019. *Jurnal Pariwisata Bisnis Digital dan Manajemen*, 1(2), 87–93.
<https://doi.org/10.33480/jasdim.v1i2.3537>

Nafi'ah, B. A. (2022). Challenges of Implementing an Electronic-Based Government System in Local Governments. *KnE Social Sciences*.
<https://doi.org/10.18502/kss.v7i9.10932>

Ningtyas, K. T., Gumilang, S. F. S., & Hanafi, R. (2023). Perancangan Arsitektur Sistem Pemerintahan Berbasis Elektronik Pada Urusan Sosial Di Pemerintah Provinsi Jawa Barat Berbasis Konsep Enterprise Architecture Menggunakan Kerangka Kerja Togaf Adm. *JIPi (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 8(2), 355–369.-
<https://doi.org/10.29100/jipi.v8i2.3454>

Purnomo, S. J. (2023). Mewujudkan Pelayanan Publik dalam Sistem Pemerintahan Berbasis Elektronik: Peran Diskominfo Provinsi Jawa Tengah Pada 2018-2023. *Bappenas Working Papers*, 6(1), 98–112.
<https://doi.org/10.47266/bwp.v6i1.189>

- Taufik, Liwaul, & Sartono. (2023). Analisis Faktor Keberhasilan Implementasi Kebijakan Sistem Pemerintahan Berbasis Elektronik Di Kabupaten Konawe Selatan. *Journal Publicuho*, 6(2), 507–524. <https://doi.org/10.35817/publicuho.v6i2.134>
- Yanuhar, U., Musa, M., Evanuarini, H., Wuragil, D. K., & Permata, F. S. (2022). Water Quality in Koi Fish (*Cyprinus carpio*) Concrete Ponds with Filtration in Nglegok District, Blitar Regency. *Universal Journal of Agricultural Research*, 10(6), 814–820. <https://doi.org/10.13189/ujar.2022.100619>

