

# Evaluasi Enterprise Risk Management Pada Lembaga Xyz Dengan Menggunakan Framework Spbe Pada Daftar Risiko Nomor 7-9, 19-21, Dan 52-64

1<sup>st</sup> Wan Liufang Bagus Candido

Fakultas Rekayasa Industri

Universitas Telkom

Bandung, Indonesia

kendibagus@student.telkomuniversity.ac.id

2<sup>nd</sup> Lukman Abdurrahman

Fakultas Rekayasa Industri

Universitas Telkom

Bandung, Indonesia

abdural@telkomuniversity.ac.id

3<sup>rd</sup> Ari Fajar Santoso

Fakultas Rekayasa Industri

Universitas Telkom

Bandung, Indonesia

arifajar@telkomuniversity.ac.id

**Abstrak** - Penelitian ini bertujuan untuk menganalisis manajemen risiko dan mengkategorikannya menjadi 3 level yaitu sangat tinggi, tinggi, dan sedang. Lalu memberikan rekomendasi terkait penanganan risiko yang terdapat pada Lembaga XYZ sehingga dapat menurunkan level risiko dari kejadian tersebut. Hasil penelitian mengkategorikan risiko menjadi 3 level yaitu sangat tinggi, tinggi, dan sedang. Selain itu penelitian ini menunjukkan bahwa pada Lembaga XYZ ini sudah memiliki sistem manajemen risiko yang cukup memadai, namun dalam beberapa kejadian masih ada bentuk penanganan risiko yang kurang efektif. Sehingga penulis menyarankan beberapa rekomendasi untuk menyempurnakan Lembaga XYZ dalam menangani sebuah risiko. Kesimpulan dari penelitian ini adalah pentingnya peningkatan dalam pelaksanaan manajemen risiko di Lembaga XYZ. Dibutuhkan usaha untuk meningkatkan pemahaman dan kemampuan sumber daya manusia terkait manajemen risiko dan juga perlu adanya fokus lebih terhadap infrastruktur yang digunakan. Selain itu, peningkatan dalam proses manajemen risiko harus selalu dilakukan supaya dampak yang ditimbulkan tidak terlalu besar. Diharapkan bahwa penelitian ini akan menjadi dasar untuk pengembangan lebih lanjut dalam manajemen risiko pada Lembaga XYZ maupun di perusahaan TI lainnya.

**Kata Kunci**— Evaluasi Risiko, Manajemen Risiko, Kategori Risiko, Penanganan Risiko, Sistem Pemerintahan Berbasis Elektronik (SPBE).

## I. PENDAHULUAN

Secara keseluruhan, ERM dapat dipahami sebagai metode yang digunakan untuk mengelola risiko secara strategis dari sudut pandang keseluruhan organisasi atau bisnis. Bersamaan, para pemimpin organisasi akan mengidentifikasi, menilai, dan mempersiapkan kerugian, potensi bahaya, dan potensi kerugian lainnya yang dapat mengganggu operasi dan tujuan organisasi. Menurut modul yang ditulis oleh Mark Beasley dari State University of New York, ERM tidak hanya diartikan sebagai pengelolaan dan pencegahan risiko yang dilakukan oleh para pemimpin organisasi agar unit

bisnisnya dapat bertahan tetapi juga tentang pengelolaan risiko yang sudah ada dalam suatu perusahaan.

Pesatnya perkembangan teknologi telah mempengaruhi berbagai aspek kehidupan manusia, baik sosial, budaya, ekonomi, politik dan hukum. Pemanfaatan teknologi juga telah mengubah pola komunikasi dan interaksi secara signifikan, bahkan dalam konteks pelayanan pemerintah kepada masyarakat. Dalam konteks pemerintahan, pemanfaatan teknologi untuk mengelola pemerintahan dan memberikan pelayanan kepada masyarakat sering disebut dengan e-Government..

Dalam studi ini, XYZ telah terpilih sebagai subjek dalam penilaian manajemen risiko. XYZ adalah sebuah badan pemerintah yang memiliki kewajiban kepada presiden dan fokusnya adalah pada riset, pengembangan, evaluasi, implementasi, serta pengembangan inovatif yang terintegrasi. Walaupun XYZ telah menerapkan manajemen risiko, namun prosesnya belum berjalan secara efektif. Proses ERM yang sedang berjalan mungkin tidak memadai atau tidak berfungsi dengan efektif dalam mengidentifikasi, mengevaluasi, dan mengurangi risiko-risiko yang ada.

## II. KAJIAN TEORI

Pada bagian landasan teori merupakan bagian penting dari sebuah karya ilmiah, dimana di dalamnya berisi tentang pengetahuan yang menjadi dasar atau landasan untuk mengkaji suatu masalah atau fenomena tertentu. Dalam bab ini, akan dipaparkan berbagai teori, konsep, dan literatur yang relevan yang akan digunakan sebagai landasan dalam menganalisis dan menginterpretasi data serta temuan dalam penelitian ini. Melalui pemahaman mendalam terhadap teori-teori yang ada, diharapkan akan membantu dalam memperkuat argumentasi dalam menjawab pertanyaan penelitian serta mencapai tujuan penelitian yang telah ditetapkan.

### A. Manajemen Risiko

Menurut (Hanafi:2009) “Risiko diklasifikasikan menjadi dua, yaitu : risiko murni dan resiko spekulatif risiko murni merupakan risiko di mana kemungkinan kerugian ada tetapi kemungkinan keuntungan tidak ada, sedangkan risiko spekulatif merupakan risiko di mana kita mengharapkan terjadinya kerugian dan juga keuntungan”. Menurut (Herman Darmawi:2006) menyatakan, “manajemen risiko adalah suatu usaha untuk mengetahui, menganalisis, serta mengendalikan risiko dalam setiap kegiatan perusahaan dengan tujuan untuk memperoleh efektivitas dan efisiensi yang lebih tinggi”. Menurut (Diyanti:2019) “mendefinisikan manajemen risiko sebagai suatu bidang ilmu yang membahas tentang bagaimana suatu organisasi atau perusahaan menerapkan ukuran dalam memetakan berbagai permasalahan yang ada dengan menempatkan berbagai pendekatan manajemen secara komprehensif dan sistematis”.

Dapat disimpulkan dari pengertian diatas, manajemen risiko adalah suatu metode yang digunakan untuk mengidentifikasi, mengukur dan mengelola penyebab dan dampak ketidakpastian dalam suatu organisasi atau bisnis. Oleh karena itu, manajemen risiko diperlukan untuk menghindari dan meminimalkan risiko yang akan timbul atau yang akan dihadapi perusahaan..

### B. Sistem Pemerintahan Berbasis Elektronik

Sistem Pemerintahan Berbasis Elektronik (SPBE) atau e-government adalah implementasi pemerintahan yang menggunakan Teknologi Informasi dan Komunikasi (TIK) untuk menyediakan layanan kepada berbagai pihak, termasuk lembaga pemerintah, Pegawai Negeri Sipil (PNS), pelaku usaha, warga, dan aktor lainnya. Penggunaan SPBE akan mendorong dan menciptakan tata kelola pemerintahan yang lebih terbuka, melibatkan partisipasi lebih banyak pihak, berinovasi, dan bertanggung jawab. Hal ini juga akan memperkuat kolaborasi antar lembaga pemerintah dalam menjalankan fungsi pemerintahan guna mencapai tujuan bersama, meningkatkan mutu serta jangkauan layanan publik untuk masyarakat secara umum, serta mengurangi insiden penyalahgunaan wewenang, seperti konspirasi, korupsi, dan nepotisme, dengan mengimplementasikan sistem pengawasan dan pelaporan masyarakat berbasis elektronik.

Bagi upaya meningkatkan inovasi dalam pembangunan aparatur negara, pemerintah menerapkan Sistem Pemerintahan Berbasis Elektronik atau e-government, yang merupakan pelaksanaan pemerintahan yang menggunakan Teknologi Informasi dan Komunikasi (TIK) untuk menyediakan layanan kepada entitas pemerintah. “SPBE adalah istilah yang digunakan untuk menggambarkan penggunaan teknologi informasi dan komunikasi untuk meningkatkan efisiensi dan efektivitas layanan pemerintah” (Arief dkk, 2021). Visi SPBE Nasional yang tertuang dalam Peraturan Presiden Nomor 95 Tahun 2018, yaitu “Terwujudnya Sistem Pemerintahan Berbasis Elektronik yang Terpadu dan Menyeluruh untuk Mencapai Birokrasi dan Pelayanan Publik yang Berkinerja Tinggi.” (Khaidarmansyah & Ridwan Saifuddin, 2022). Aparatur Sipil Negara (ASN), pelaku usaha, masyarakat dan pihak lainnya. Penyelenggaraan SPBE akan mendorong dan mewujudkan penyelenggaraan pemerintahan yang terbuka, partisipatif, inovatif dan bertanggung jawab, meningkatkan kerjasama antar instansi pemerintah dalam melaksanakan tugas dan

tanggung jawab pelayanan pemerintah untuk mencapai tujuan bersama, meningkatkan mutu dan cakupan pelayanan kepada masyarakat luas dan kemauan mengurangi tingkat penyalahgunaan kekuasaan berupa kolusi, korupsi dan nepotisme melalui penerapan sistem pengaduan dan pemantauan masyarakat secara elektronik.

Manfaat penerapan manajemen risiko SPBE dalam penerapan SPBE adalah:

1. Mewujudkan penyelenggaraan pemerintahan yang efektif, efisien, transparan, dan akuntabel melalui penerapan SPBE pada otoritas pusat dan daerah;
2. Mewujudkan pengarusutamaan SPBE pada otoritas pusat dan daerah;
3. Meningkatkan kinerja pemerintahan pada instansi pemerintah pusat dan daerah;
4. Meningkatkan kredibilitas dan kepercayaan pemangku kepentingan terhadap instansi pemerintah pusat dan daerah;
5. Menciptakan budaya kerja profesionalisme dan integritas pada instansi pemerintah pusat dan daerah.

### C. Kerangka Kerja Manajemen Risiko SPBE

Kerangka manajemen risiko SPBE menguraikan unsur-unsur mendasar yang dijadikan landasan dalam penerapan manajemen risiko SPBE pada instansi pemerintah pusat dan daerah. Tujuan kerangka manajemen risiko SPBE adalah untuk membantu otoritas pusat dan daerah dalam mengintegrasikan manajemen risiko SPBE ke dalam kegiatan yang bertujuan untuk melaksanakan tugas dan fungsi otoritas pusat dan daerah. Agar manajemen risiko SPBE dapat terlaksana dengan baik, instansi pusat dan pemerintah daerah dapat langsung mengadopsi atau memodifikasi kerangka manajemen risiko SPBE sesuai dengan konteks internal dan eksternal lingkungan masing-masing. Elemen mendasar dari kerangka ini mencakup prinsip-prinsip yang terkait dengan peningkatan dan perlindungan nilai, kepemimpinan dan komitmen, integrasi, perbaikan, desain, implementasi, pemantauan dan evaluasi, serta budaya sadar risiko.



Gambar II. 1  
Kerangka Kerja Manajemen Risiko SPBE

1. Peningkatan Nilai dan Perlindungan merupakan Prinsip dasar penerapan manajemen risiko SPBE dengan menciptakan nilai dan perlindungan yang lebih besar bagi pemerintahan pusat dan Pemerintah daerah dalam pelaksanaan SPBE.

2. Kepemimpinan dan Komitmen dari pimpinan pemerintah pusat dan daerah harus menunjukkan kepemimpinan dan keterlibatan dalam penerapan sistem manajemen risiko SPBE

### III. METODOLOGI PENELITIAN

Metode penelitian yang digunakan adalah metode kualitatif. Penelitian kualitatif merupakan jenis penelitian yang berupaya memperoleh pemahaman mendalam mengenai fenomena sosial, dengan menggunakan teknik pengumpulan data non numerik. Cara ini termasuk wawancara mendalam, observasi partisipatif, dan analisis dokumen. Penelitian kualitatif biasanya mengkonsentrasikan pada satu atau beberapa unit analisis, seperti individu, kelompok kecil, atau organisasi. Hasil penelitian kualitatif biasanya ditafsirkan dalam bentuk naratif atau deskriptif. Penelitian kualitatif sangat berguna untuk memberikan pemahaman yang lebih dalam tentang bagaimana orang-orang mengalami dan memahami dunia mereka, terutama dalam konteks sosial yang kompleks.

#### A. Metode Pengumpulan Data

Metode pengumpulan data dengan SPBE (Sistem Pemerintahan Berbasis Elektronik) berupa studi buku, publikasi, dan elektronik adalah pendekatan yang dilakukan untuk mengumpulkan informasi dan data dengan cara menggunakan sumber-sumber tertulis seperti buku, jurnal ilmiah, publikasi, dokumen elektronik, dan konten digital lainnya. Pendekatan ini digunakan dalam penelitian atau studi yang memerlukan data sekunder atau informasi yang sudah ada dan dipublikasikan sebelumnya. Metode SBPE memungkinkan peneliti untuk memanfaatkan pengetahuan yang telah dikumpulkan oleh penulis sebelumnya atau lembaga yang telah melakukan penelitian sebelumnya, tanpa perlu mengumpulkan data dari lapangan secara langsung.

Dalam menggunakan metode SBPE, peneliti perlu melakukan langkah-langkah tertentu. Pertama, identifikasi sumber-sumber yang relevan dan terpercaya yang sesuai dengan tujuan penelitian. Kedua, peneliti harus menganalisis dan mengevaluasi kualitas serta keakuratan data yang ada dalam sumber-sumber tersebut. Selain itu, diperlukan keterampilan kritis untuk menilai kehandalan dan objektivitas penulis atau lembaga yang telah menyediakan data. Meskipun metode SBPE dapat memberikan akses yang lebih mudah terhadap data yang ada, peneliti juga harus berhati-hati dalam memeriksa validitas dan relevansi informasi agar hasil penelitian menjadi akurat dan terpercaya.

#### 1. Data Primer

Wawancara adalah salah satu metode pengumpulan data yang digunakan dalam penelitian. Wawancara merupakan cara bertanya dan mendapatkan jawaban langsung dari responden. Wawancara dapat dilakukan secara lisan atau tertulis, tergantung pada kebutuhan peneliti dan kondisi responden. "Wawancara digunakan sebagai teknik pengumpulan data apabila ingin melakukan studi pendahuluan untuk menemukan permasalahan yang harus diteliti, dan juga apabila peneliti ingin mengetahui hal-hal dari responden yang lebih mendalam dan jumlah respondennya sedikit/kecil" (Sugiono, 2018).

Wawancara dapat digunakan untuk mengumpulkan data yang lebih mendalam dan terperinci daripada metode lainnya, seperti kuesioner atau angket. Wawancara juga dapat digunakan untuk mengumpulkan data yang tidak dapat diperoleh dengan metode lainnya, seperti perasaan, pemikiran, atau motivasi responden.

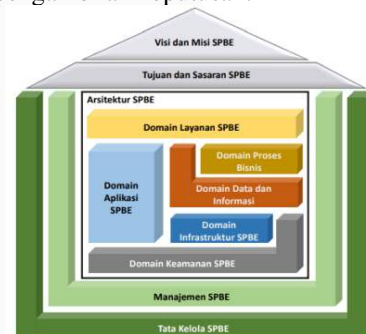
#### 2. Data Sekunder

Studi pustaka adalah salah satu metode pengumpulan data yang digunakan dalam penelitian. Studi pustaka adalah proses mengumpulkan informasi dari sumber-sumber tertulis, seperti buku, jurnal, artikel ilmiah, dan dokumen resmi lainnya. Studi pustaka dilakukan untuk mengumpulkan informasi tentang teori, konsep, atau fakta yang telah diperoleh oleh para ahli di bidang terkait. "Metode yang digunakan dalam kajian ini menggunakan metode atau pendekatan kepustakaan (library research), Studi pustaka atau kepustakaan dapat diartikan sebagai serangkaian kegiatan yang berkenaan dengan metode pengumpulan data pustaka, membaca dan mencatat serta mengolah bahan penelitian" (Supriyadi, 2017).

Studi pustaka adalah proses mengumpulkan informasi dari sumber-sumber tertulis, seperti buku, jurnal, artikel ilmiah, dan dokumen resmi lainnya. Studi pustaka dilakukan untuk mengumpulkan informasi tentang teori, konsep, atau fakta yang telah diperoleh oleh para ahli di bidang terkait. "Bahan pustaka yang didapat dari berbagai referensi tersebut dianalisis secara kritis dan harus mendalam agar dapat mendukung proposisi dan gagasannya" (Adlini dkk, 2022).

#### B. Kerangka Konseptual

Kerangka konseptual dipakai buat menyusun pemahaman yang lebih sistematis mengenai suatu fenomena atau topik tertentu, membantu mengidentifikasi interaksi antara elemen-elemen yg terlibat, & menaruh landasan bagi analisis lebih lanjut atau pengambilan keputusan.



Gambar III. 1

Kerangka Konseptual (Penyusunan Domain Arsitektur SPBE)

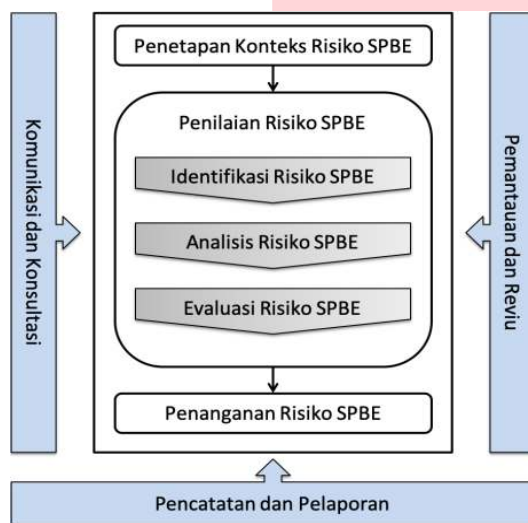
Salah satu komponen utama dalam kerangka SPBE adalah Arsitektur SPBE yang merupakan pedoman integrasi dalam tata kelola. Fungsi Arsitektur SPBE adalah melakukan pemantauan dan evaluasi kegiatan penyelenggaraan pemerintahan secara terpadu dan menyeluruh di semua bidang dan tingkatan. Kerangka SPBE menjadi landasan bagi Kerangka Arsitektur SPBE Nasional dalam pelaksanaan dan pengelolaan sistem pemerintahan pusat dan daerah. Kerangka Arsitektur SPBE berfungsi sebagai panduan untuk membangun layanan pemerintah berbasis elektronik yang terintegrasi, menghilangkan tumpang tindih dalam pelaksanaan proses bisnis, dan memastikan penerapan data

dan informasi bersama ke dalam Satu Data Indonesia melalui dukungan teknologi informasi dan komunikasi bersama yang terintegrasi. Gambar II.2 merupakan penggambaran dari kerangka arsitektur SPBE berdasarkan Perpres Tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional. (Perpres Tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional, 2021).

#### IV. OBJEK PENELITIAN

##### A. Proses Manajemen Risiko SPBE

Ini adalah seperangkat kebijakan, prosedur dan praktik untuk layanan komunikasi dan konsultasi, perencanaan situasional, analisis risiko (identifikasi risiko, analisis risiko, evaluasi risiko), manajemen risiko, pemantauan dan evaluasi, serta pencatatan dan pelaporan. Sistem manajemen risiko SPBE disajikan pada gambar IV.1 berikut.



Gambar IV. 1  
Proses Manajemen Risiko

Penjelasan gambar :

##### A. Komunikasi dan konsultasi

Komunikasi dan konsultasi adalah sebuah proses terus menerus dan berulang kali memberi, berbagi atau mendapatkan informasi dan menciptakan dialog antar pemangku kepentingan tentang risiko SPBE. Jenis layanan komunikasi dan konsultasi antara lain:

1. Rapat rutin adalah rapat selalu terorganisir;
2. Rapat insidental adalah pertemuan yang dilakukan sewaktu-waktu; Dan
3. Focus Group Discussion (FGD), yaitu Kelompok fokus yang dirancang untuk mendiskusikan topik tertentu.

##### B. Penetapan Konteks Risiko SPBE

Tujuan dari penetapan konteks risiko SPBE adalah mengidentifikasi elemen kunci dan ruang lingkup penerapan risiko SPBE yang akan dikelola dalam sistem manajemen risiko SPBE.

##### C. Penilaian Risiko SPBE

Evaluasi risiko SPBE dalam pelaksanaan SPBE dilakukan dengan melakukan tahapan identifikasi, analisis, dan penilaian risiko SPBE. Tujuan dari penilaian risiko SPBE adalah untuk memahami potensi serta konsekuensi risiko

SPBE yang mungkin terjadi pada lembaga pemerintahan pusat dan daerah.

Tahapan penilaian Risiko SPBE meliputi:

##### 1. Identifikasi Risiko SPBE

Identifikasi risiko SPBE adalah sebuah proses meninjau informasi kejadian, penyebab dan dampak bahaya SPBE.

Informasi yang didapat meliputi:

##### A. Jenis Risiko SPBE

Risiko dalam Sistem Pemerintahan berbasis elektronik (SPBE) terbagi menjadi dua kategori, yaitu risiko SPBE yang bersifat positif dan risiko SPBE yang bersifat negatif. Ketika melakukan identifikasi risiko SPBE, risiko dicatat pada kategori yang sesuai..

##### B. Kejadian dapat diidentifikasi

melalui terjadinya suatu kejadian yang mengakibatkan diperolehnya risiko SPBE yang didapat dari sejarah kejadian dan/atau prediksi kejadian di masa depan. Kejadian selanjutnya disebut Risiko SPBE.

##### C. Penyebab

Penyebab dapat diidentifikasi akar permasalahan yang menyebabkan munculnya risiko SPBE. Dapat berasal dari lingkungan internal dan eksternal lembaga pusat dan pemerintah Daerah. Mengetahui penyebabnya akan membantu menemukan tindakan yang tepat mengelola risiko SPBE.

##### D. Kategori

Penetapan Kategori Risiko SPBE dilakukan dengan tujuan untuk memastikan bahwa identifikasi, analisis, dan evaluasi Risiko SPBE dilaksanakan secara komprehensif. Kategori risiko dalam semua ringkasan risiko diidentifikasi sesuai dengan jenis risiko yang muncul.

##### E. Dampak

Dampak dapat diketahui dari pengaruh atau akibat dari Risiko SPBE.

##### F. Area Dampak

Penetapan area dampak dari Risiko SPBE bertujuan untuk mengidentifikasi daerah-daerah yang mungkin terdampak oleh Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. Proses ini dimulai dengan mengidentifikasi dampak yang mungkin timbul akibat Risiko SPBE..

##### 2. Analisis Risiko SPBE

Analisis risiko SPBE adalah suatu proses untuk melakukan peninjauan terhadap risiko SPBE yang telah diidentifikasi sebelumnya. Penilaian risiko SPBE dilakukan dengan menentukan tindakan pengendalian, tingkat probabilitas dan tingkat dampak terjadinya risiko SPBE.

##### 3. Evaluasi Risiko SPBE

Evaluasi risiko SPBE dilakukan untuk membuat keputusan apakah akan mengambil tindakan manajemen risiko atau tidak serta penetapan prioritas penanganannya yang diperlukan.

##### D. Penanganan Risiko SPBE

Penanganan risiko SPBE melibatkan proses mengubah faktor-faktor risiko SPBE. Proses ini melibatkan identifikasi opsi yang dapat diambil dan pemilihan satu atau beberapa solusi untuk mengatasi risiko SPBE tersebut..

Opsi Penanganan Risiko Negatif :

##### a) Eskalasi Risiko

Eskalasi risiko dipilih jika risiko SPBE berada di luar atau melebihi wewenang. Pilihan ini dibuat dengan memindahkan

tanggung jawab penanganan manajemen risiko SPBE kepada sektor-sektor yang berkinerja lebih tinggi.

b) Mitigasi Risiko

Mitigasi risiko ini dilakukan dengan mengurangi tingkat peluang dan/atau tingkat pengaruh dari Risiko SPBE.

c) Transfer Risiko

Transfer risiko lebih diutamakan jika ada kemungkinan kurangnya sumber daya untuk mengelola Risiko SPBE. Pilihan ini dibuat dengan cara mentransfer kepemilikan risiko kepada orang lain untuk dipenuhi pengelolaan dan pertanggungjawaban terhadap Risiko SPBE.

d) Penghindaran Risiko

Penghindaran risiko dilakukan dengan mengubah rencana, anggaran, program dan kegiatan, atau aspek lainnya untuk memenuhi tujuan SPBE.

e) Penerimaan Risiko

Penerimaan risiko dipilih jika biaya penanganan lebih tinggi daripada manfaat yang diperoleh dari penanganan tersebut. Opsi ini dibuat dengan membiarkan risiko tersebut terjadi

Tabel IV. 1 Matriks Analisis Risiko SPBE & Level Risiko

Matriks Analisis Risiko 5 x 5			Level Dampak				
			1	2	3	4	5
			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
5	Hampir pasti terjadi	9	15	18	23	25	
4	Sering terjadi	6	12	16	19	24	
3	Kadang-Kadang terjadi	4	10	14	17	22	
2	Jarang terjadi	2	7	11	13	21	
1	Hampir tidak terjadi	1	3	5	8	20	

E. Pemantauan dan Reviu

Maksud dari pemantauan adalah untuk mengkaji faktor-faktor yang berdampak pada Risiko SPBE dan situasi pemerintahan di tingkat pusat dan daerah. Selain itu, pemantauan juga bertujuan untuk menilai bagaimana rencana penanganan Risiko SPBE dijalankan. Hasil dari pemantauan ini dapat digunakan sebagai landasan untuk melakukan perubahan dalam Sistem Manajemen Risiko SPBE.

F. Pencatatan dan Pelaporan

pencatatan adalah suatu program atau proses pencatatan peristiwa secara tertulis dan ditampilkan dalam buku. Laporan adalah tindakan yang dilakukan untuk menyampaikan terkait hasil pekerjaan yang dilakukan dalam jangka waktu tertentu.

1. Komunikasi dan Konsultasi

Proses berkelanjutan yang sering terjadi adalah komunikasi dan konsultasi yang bertujuan untuk memberikan, berbagi, atau menerima informasi guna menciptakan dialog dengan pemangku kepentingan mengenai risiko SPBE. Tujuan komunikasi adalah meningkatkan kesadaran dan pemahaman terhadap risiko SPBE.

2. Penetapan Konteks Risiko SPBE

Penetapan konteks Risiko SPBE bertujuan untuk mengenali elemen-elemen kunci serta cakupan dari Risiko SPBE yang harus diurus dalam kerangka Manajemen Risiko SPBE..

Matriks analisis risiko SPBE digunakan untuk menggabungkan tingkat probabilitas dengan tingkat dampak untuk menentukan Jumlah risiko SPBE yang dapat direpresentasikan dalam bentuk angka. Besaran risiko SPBE dikelompokkan ke dalam level risiko SPBE, dimana masing-masing tingkatannya mempunyai nilai-nilai tertentu. Pemilihan tingkat risiko SPBE dapat dilakukan menggunakan level 3, level 4, level 5 atau level lain yang sesuai dan kompleksitas risiko SPBE. Tiap tingkatan ini dapat diwakili dengan mengubah warna sesuai preferensi Instansi Pusat dan pemerintahan daerah.

B. Penilaian Risiko

Penilaian risiko merujuk pada proses sistematis untuk mengidentifikasi potensi bahaya atau ancaman yang dapat menyebabkan kerugian atau dampak negatif pada suatu perusahaan. Tujuan dari penilaian risiko adalah untuk mengidentifikasi potensi risiko, menilai tingkat dampaknya, dan menyusun langkah-langkah pengendalian atau mitigasi untuk mengurangi dampaknya.

1. Level Risiko Sangat Tinggi

Pada objek penelitian yang kami teliti level risiko sangat tinggi merupakan risiko yang memiliki nilai 20-25

Tabel IV. 2 Risiko kebakaran

Sasaran SPBE	Tersedianya data citra satelit resolusi rendah, citra satelit resolusi menengah, citra satelit resolusi tinggi, citra satelit resolusi sangat tinggi, Data Satelit Radar, dan Data Satelit Mosaik
Indikator Kinerja SPBE	Pemanfaatan data citra satelit resolusi rendah, citra satelit resolusi menengah, citra satelit resolusi tinggi, citra satelit resolusi sangat tinggi, Data Satelit Radar, dan Data Satelit Mosaik oleh masyarakat
Sumber Risiko	Pusat data/ OR PA
Kejadian	Kebakaran
Penyebab	Sistem anti kebakaran tak berfungsi, sistem dan teknis telah absolute
Dampak	Kerusakan komponen hardware di DataCenter
Kemungkinan	1 (Tidak pernah Terjadi)
Dampak Risiko	5 (Sangat signifikan)
Besaran Risiko	20
Level Risiko	Sangat Tinggi
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	Melakukan move infrastruktur SPBE

Tabel IV. 3

Risiko kepemimpinan dan pengorganisasian SPBE tidak berjalan

Sasaran SPBE	Transformasi digital perusahaan yang terintegrasi
Indikator Kinerja SPBE	Indeks SPBE perusahaan
Sumber Risiko	Kebijakan
Kejadian	Kepemimpinan dan pengorganisasian SPBE tidak berjalan
Penyebab	Tidak dipatuhinya kebijakan kepemimpinan dan organisatoris pelaksana SPBE
Dampak	Terganggunya dan tidak optimalnya organisasi SPBE
Kemungkinan	1 (Hampir tidak Terjadi)
Dampak Risiko	5 (Sangat signifikan)
Besaran Risiko	20
Level Risiko	<b>Sangat Tinggi</b>
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	Penyelenggaraan Sosialisasi dan awares

Tabel IV. 5

Risiko keteledoran personil terhadap pengamanan data dan informasi

Sasaran SPBE	Transformasi digital perusahaan yang terintegrasi
Indikator Kinerja SPBE	Indeks SPBE perusahaan
Sumber Risiko	Kebijakan
Kejadian	Personil teledor terhadap pengamanan data dan informasi
Penyebab	Tidak dipatuhinya kebijakan awareness keamanan data dan informasi
Dampak	Terganggunya sistem keamanan data dan informasi
Kemungkinan	2 (Kadang kadang terjadi)
Dampak Risiko	4 (Signifikan)
Besaran Risiko	17
Level Risiko	<b>Tinggi</b>
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	Mengadakan peningkatan awares secara berkala

Tabel IV. 4

Risiko aplikasi penginderaan jauh tidak dapat diakses

Sasaran SPBE	Aplikasi Penginderaan Jauh (citra satelit resolusi rendah, citra satelit resolusi menengah, citra satelit resolusi tinggi, citra satelit resolusi sangat tinggi, Data Satelit Radar, Data Satelit Mosaik)
Indikator Kinerja SPBE	Pemanfaatan data citra satelit resolusi rendah, citra satelit resolusi menengah, citra satelit resolusi tinggi, Data Satelit Radar, dan Data Satelit Mosaik oleh masyarakat
Sumber Risiko	Pusat data/ OR PA
Kejadian	Aplikasi penginderaan jauh tidak dapat diakses
Penyebab	Server rusak pada komponen-nya
Dampak	Aplikasi penginderaan jauh berhenti, Layanan Broadcast Digital tidak bekerja
Kemungkinan	1 (Hampir tidak Terjadi)
Dampak Risiko	5 (Sangat signifikan)
Besaran Risiko	20
Level Risiko	<b>Sangat Tinggi</b>
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	pengadaan back up hardisk

Tabel IV. 6

Risiko personil kurang mampu memberikan pelayanan prima

Sasaran SPBE	Transformasi digital perusahaan yang terintegrasi
Indikator Kinerja SPBE	Indeks SPBE perusahaan
Sumber Risiko	Kebijakan
Kejadian	Personil kurang mampu memberikan pelayanan prima
Penyebab	Tidak dipatuhinya kebijakan pengelolaan kinerja personil SPBE
Dampak	Layanan SPBE tidak optimal
Kemungkinan	2 (Kadang kadang terjadi)
Dampak Risiko	4 (Signifikan)
Besaran Risiko	17
Level Risiko	<b>Tinggi</b>
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	Evaluasi kinerja secara berkala

Tabel IV. 7

Risiko personil kurang terkendali dalam mengakses aset yang sensitif

Sasaran SPBE	Transformasi digital perusahaan yang terintegrasi
Indikator Kinerja SPBE	Indeks SPBE perusahaan
Sumber Risiko	Kebijakan
Kejadian	Personil kurang terkendali dalam mengakses aset yang sensitif
Penyebab	Tidak dipatuhinya kebijakan penggunaan dan pemanfaatan oleh pihak ke tiga
Dampak	Keamanan SPBE tidak terjamin
Kemungkinan	2 (Kadang kadang terjadi)
Dampak Risiko	4 (Signifikan)
Besaran Risiko	17
Level Risiko	<b>Tinggi</b>
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	Evaluasi kinerja personil pihak ke tiga secara berkala

2. Level Risiko Tinggi

Pada objek penelitian yang kami teliti level risiko sangat tinggi merupakan risiko yang memiliki nilai 16-19

### 3. Level Risiko Sedang

Pada objek penelitian yang kami teliti level risiko sedang merupakan risiko yang memiliki nilai 11-15

Tabel IV. 8  
Risiko tidak ada rekanan

Sasaran SPBE	Penerapan jaringan intra diseluruh unit kerja perusahaan
Indikator Kinerja SPBE	Perangkat jaringan yang berfungsi maksimal
Sumber Risiko	Jaringan Intra Pemerintah
Kejadian	Tidak ada rekanan
Penyebab	Tidak ada kebijakan yang mengatur kerjasama/kontrak
Dampak	Layanan TI tidak bisa terpenuhi secara maksimal
Kemungkinan	2 (Jarang terjadi)
Dampak Risiko	4 (Signifikan)
Besaran Risiko	13
Level Risiko	Sedang
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	Melakukan evaluasi kebijakan terkait penyelenggaraan kerjasama/kontrak rekanan ISP

Tabel IV. 9  
Risiko sistem layanan terinfeksi virus dan/atau malware

Sasaran SPBE	Layanan perusahaan yang efektif dan efisien
Indikator Kinerja SPBE	Tingkat layanan TI perusahaan
Sumber Risiko	Sistem Layanan/ELSA
Kejadian	Sistem layanan terinfeksi virus dan/atau malware
Penyebab	1. Belum dilakukan update dan patching pada sistem operasi secara konsisten 2. Belum semua server pada DC terinstall antivirus
Dampak	Hilangnya data baik pada server maupun user
Kemungkinan	2 (Jarang terjadi)
Dampak Risiko	4 (Signifikan)
Besaran Risiko	13
Level Risiko	Sedang
Opsi penanganan Risiko	Reduce Risk
Rencana Aksi Penanganan Risiko SPBE	1. Melakukan backup dan sinkronisasi 2. Pemantauan instalasi antivirus terhadap perangkat server

Tabel IV. 10

Risiko sistem Layanan Mengalami Gangguan / Tidak dapat diakses.

Sasaran SPBE	Layanan perusahaan yang efektif dan efisien
Indikator Kinerja SPBE	Tingkat layanan TI perusahaan
Sumber Risiko	Sistem Layanan/ELSA
Kejadian	Sistem Layanan Mengalami Gangguan / Tidak dapat diakses.
Penyebab	Server tidak bisa mengakomodir kebutuhan masyarakat, terlalu banyak user yang mengakses dalam satu waktu bersamaan
Dampak	Downtime terhadap layanan / Aplikasi
Kemungkinan	2 (Jarang terjadi)
Dampak Risiko	4 (Signifikan)
Besaran Risiko	13
Level Risiko	Sedang
Opsi penanganan Risiko	Reduce Risk
Rencana Aksi Penanganan Risiko SPBE	1. Menyusun kajian kapasitas optimal perangkat monitoring 2. Menindaklanjuti hasil monitoring

Tabel IV. 11

Risiko perangkat jaringan tidak berfungsi /terganggu

Sasaran SPBE	Penerapan jaringan intra diseluruh unit kerja perusahaan
Indikator Kinerja SPBE	Perangkat jaringan yang berfungsi maksimal
Sumber Risiko	Jaringan Intra Pemerintah
Kejadian	Perangkat jaringan tidak berfungsi /terganggu
Penyebab	Kerusakan perangkat, Terdapat perangkat yang menjadi <i>Single Point of failure (SPOF)</i> , Perangkat sudah <i>end of support/obsolete</i> , Perangkat sudah <i>end of support/obsolete</i> , <i>Monitoring</i> perangkat tidak optimal
Dampak	Koneksi jaringan internet dan/atau intranet lambat dan/atau terputus.
Kemungkinan	2 (Jarang terjadi)
Dampak Risiko	3 (Cukup Signifikan)
Besaran Risiko	11
Level Risiko	Sedang
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	Pelaksanaan pengecekan rutin perangkat jaringan

TABEL IV. 12  
 Risiko Gangguan / Kerusakan perangkat jaringan Core Gedung

Sasaran SPBE	Penerapan jaringan intra diseluruh unit kerja perusahaan
Indikator Kinerja SPBE	Perangkat jaringan yang berfungsi maksimal
Sumber Risiko	Jaringan Intra Pemerintah
Kejadian	Gangguan / Kerusakan perangkat jaringan Core Gedung
Penyebab	Kerusakan perangkat ( <i>Module, Port, OS</i> ), perangkat <i>end of support</i> , Kondisi ruangan belum optimal (misalnya: Panas , kotor, letak yang tidak sesuai, dll), Monitoring Perangkat tidak optimal
Dampak	Koneksi jaringan terhenti/terhambat
Kemungkinan	2 (Jarang terjadi)
Dampak Risiko	3 (Cukup Signifikan)
Besaran Risiko	11
Level Risiko	Sedang
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	Pelaksanaan pengecekan rutin perangkat jaringan

TABEL IV. 13  
 Risiko kabel putus

Sasaran SPBE	Penerapan jaringan intra diseluruh unit kerja perusahaan
Indikator Kinerja SPBE	Perangkat jaringan yang berfungsi maksimal
Sumber Risiko	Jaringan Intra Pemerintah
Kejadian	Kabel putus
Penyebab	Rusak karena hewan hama (digigit tikus)
Dampak	Pekerjaan terkait transaksi data/layanan online terganggu
Kemungkinan	2 (Jarang terjadi)
Dampak Risiko	3 (Cukup Signifikan)
Besaran Risiko	11
Level Risiko	Sedang
Opsi penanganan Risiko	Mitigasi
Rencana Aksi Penanganan Risiko SPBE	Penerapan SOP terkait

V. ANALISIS DAN HASIL PENGUJIAN

A. Gap Analysis

Gap analysis adalah suatu metode yang digunakan untuk membandingkan dan menganalisis perbedaan atau kesenjangan antara kondisi atau performa yang ada dengan kondisi atau performa yang diharapkan atau diinginkan. Tujuan dari gap analysis adalah untuk mengidentifikasi kesenjangan atau celah antara apa yang telah dicapai saat ini dan apa yang seharusnya dicapai.

1. Gap Analisis Level Risiko Sangat Tinggi

TABEL V. 1  
 Gap Analisis Level Risiko : Sangat Tinggi

Requirement	Fulfillment			Keterangan	Solusi Alternatif
	N	P	F		
Meminimalisir kerusakan komponen hardware di DataCenter		✓		Kerusakan komponen hardware di DataCenter	Permintaan penyediaan backup dilokasi lain
Optimalnya organisasi SPBE		✓		Terganggunya dan tidak optimalnya organisasi SPBE	Melaksanakan transformasi digital yang sudah diinstruksikan
Aplikasi penginderaan jauh dan layanan broadcast digital selalu bekerja		✓		Aplikasi penginderaan jauh berhenti, Layanan broadcast Digital tidak bekerja	Menyediakan perangkat backup

2. Gap Analisis Level Risiko Tinggi

TABEL V. 2  
 Gap Analisis Level Risiko Tinggi

Requirement	Fulfillment			Keterangan	Solusi Alternatif
	N	P	F		
Sistem keamanan data dan informasi yang stabil		✓		Terganggunya sistem keamanan data dan informasi	Peningkatan kesadaran pentingnya keamanan SPBE secara berkala
Pengoptimalan layanan SPBE		✓		Layanan SPBE tidak optimal	Evaluasi kinerja secara berkala
Terjamin nya system keamanan SPBE		✓		Keamanan SPBE tidak terjamin	Melakukan tinjauan ulang SOP yang berkaitan hak akses aset

B. Rekomendasi

Pada bagian Rekomendasi, penulis ingin mengusulkan beberapa langkah tindakan yang dapat diambil untuk mengatasi permasalahan yang telah diidentifikasi sebelumnya.

1. Rekomendasi Level Risiko Sangat Tinggi

TABEL V. 3  
 Rekomendasi terjadi nya kebakaran

Kejadian	Kebakaran
Penyebab	Sistem anti kebakaran tak berfungsi, sistem dan teknis telah absolute
Dampak	- Kerusakan komponen hardware di DataCenter - <b>Kehilangan data dan informasi</b>
Kemungkinan	1 (Tidak pernah Terjadi)
Dampak risiko	5 (Sangat signifikan)
Besaran risiko	20
Level Risiko	<b>Sangat Tinggi</b>
Opsi penanganan risiko	Mitigasi
Rencana aksi penanganan risiko SPBE	- Melakukan monev infrastruktur SPBE - <b>Kerjasama dengan pihak eksternal</b> - <b>Pemantauan keamanan</b>

Keterangan: Tulisan Bold Merupakan Hasil Rekomendasi Dari Hasil Penelitian

Pada bagian dampak, penulis menambahkan dampak yang mungkin terjadi jika kebakaran tersebut terjadi yaitu



kehilangan data dan informasi karena Lembaga XYZ menyimpan data penelitian, informasi, dan inovasi penting dalam bentuk fisik maupun digital. Jika data ini rusak atau hancur akibat kebakaran, hal ini dapat menyebabkan kehilangan pengetahuan berharga dan potensial terhentinya proyek penelitian yang sedang berlangsung.

Pada bagian rencana aksi penanganan risiko penulis menambahkan kerjasama dengan pihak eksternal seperti pemadam kebakaran setempat dan Lembaga keamanan sehingga pihak eksternal tersebut bisa cepat tanggap jika terjadi kebakaran pada Lembaga XYZ. Selain itu, rencana aksi penanganan lainnya adalah pemantauan keamanan yaitu dengan menerapkan sistem pemantauan keamanan yang bisa melakukan pemantauan terhadap kebakaran dan gas sehingga membantu mendeteksi potensi ancaman sejak dini.

TABEL V. 4  
Rekomendasi kepemimpinan dan pengorganisasian SPBE tidak berjalan

Kejadian	Kepemimpinan dan pengorganisasian SPBE tidak berjalan
Penyebab	Tidak dipatuhinya kebijakan kepemimpinan dan organisatoris pelaksana SPBE
Dampak	- Terganggunya dan tidak optimalnya organisasi SPBE - <b>Kurangnya Kolaborasi dan Sinergi</b>
Kemungkinan	1 (Hampir tidak Terjadi)
Dampak risiko	5 (Sangat signifikan)
Besaran risiko	20
Level Risiko	<b>Sangat Tinggi</b>
Opsi penanganan risiko	Mitigasi
Rencana aksi penanganan risiko SPBE	- Penyelenggaraan Sosialisasi dan awareness - <b>Pengembangan Tim dan Keterlibatan Karyawan</b> - <b>Kolaborasi dan Komunikasi</b>

Keterangan: Tulisan Bold Merupakan Hasil Rekomendasi Dari Hasil Penelitian

Pada bagian dampak, penulis menambahkan kurangnya kolaborasi dan sinergi karena tanpa kepemimpinan yang baik, kolaborasi antarunit pada Lembaga XYZ mungkin sulit terwujud. Padahal, kolaborasi dan sinergi antara berbagai departemen atau lembaga riset adalah kunci untuk menciptakan inovasi yang lebih kuat dan penemuan ilmiah yang lebih bermakna.

Pada bagian rencana aksi penanganan risiko penulis menambahkan pengembangan tim dan keterlibatan karyawan hal tersebut bisa dilakukan dengan memberikan kesempatan kepada setiap karyawan untuk berpartisipasi dalam proyek-proyek inovatif. Selain itu, rencana aksi penanganan lainnya adalah dengan kolaborasi dan komunikasi hal tersebut bisa di dorong dengan melakukan komunikasi yang terbuka di antara semua anggota lembaga untuk meningkatkan sinergi dan pencapaian tujuan bersama.

TABEL V. 5

Rekomendasi aplikasi penginderaan jauh tidak dapat diakses

Kejadian	Aplikasi penginderaan jauh tidak dapat diakses
Penyebab	Server rusak pada komponennya
Dampak	- Aplikasi penginderaan jauh berhenti, Layanan Broadcast Digital tidak bekerja - <b>Gangguan pada proyek penelitian</b>
Kemungkinan	1 (Hampir tidak Terjadi)
Dampak risiko	5 (Sangat signifikan)
Besaran risiko	20
Level Risiko	<b>Sangat Tinggi</b>
Opsi penanganan risiko	Mitigasi
Rencana aksi penanganan risiko SPBE	- pengadaan back up hardisk - <b>Diversifikasi sumber data</b>

Keterangan: Tulisan Bold Merupakan Hasil Rekomendasi Dari Hasil Penelitian

Pada bagian dampak penulis menambahkan gangguan pada proyek penelitian karena banyak proyek penelitian pada Lembaga XYZ mengandalkan data penginderaan jauh untuk analisis dan pemodelan. Jika akses ke data ini terganggu, proyek-proyek ini mungkin mengalami keterlambatan atau bahkan gagal untuk mencapai tujuan penelitian yang telah ditetapkan.

Pada bagian rencana aksi penanganan penulis menambahkan diversifikasi sumber data yaitu dengan cara Lembaga harus mencari alternatif sumber data penginderaan jauh untuk mengatasi risiko ketidakmampuan akses. Ini dapat berupa kesepakatan dengan lembaga atau satelit lain yang menyediakan data serupa.

## 2. Rekomendasi Level Risiko Tinggi

TABEL V. 6

Rekomendasi keteledoran personil terhadap pengamanan data dan informasi

Kejadian	Personil teledor terhadap pengamanan data dan informasi
Penyebab	Tidak dipatuhinya kebijakan awareness keamanan data dan informasi
Dampak	- Terganggunya sistem keamanan data dan informasi - <b>Hilangnya kepercayaan</b>
Kemungkinan	2 (Kadang kadang terjadi)
Dampak risiko	4 (Signifikan)
Besaran risiko	17
Level Risiko	<b>Tinggi</b>
Opsi penanganan risiko	Mitigasi
Rencana aksi penanganan risiko SPBE	- Mengadakan peningkatan awareness secara berkala - <b>Audit Keamanan</b>

Keterangan: Tulisan Bold Merupakan Hasil Rekomendasi Dari Hasil Penelitian

Pada bagian dampak penulis menambahkan hilangnya kepercayaan hal tersebut dikarenakan keteledoran dalam pengamanan data dan informasi dapat merusak kepercayaan mitra, masyarakat, dan lembaga lain terhadap instansi. Hilangnya kepercayaan ini dapat berdampak buruk pada kolaborasi dan reputasi organisasi.

Pada bagian rencana aksi penanganan risiko penulis menyarankan untuk melakukan audit keamanan secara berkala untuk mengevaluasi kepatuhan dan efektivitas kebijakan keamanan serta mengidentifikasi area yang memerlukan perbaikan.

TABEL V. 7

Rekomendasi personil kurang mampu memberikan pelayanan prima

Kejadian	Personil kurang mampu memberikan pelayanan prima
Penyebab	Tidak dipatuhinya kebijakan pengelolaan kinerja personil SPBE
Dampak	- Layanan SPBE tidak optimal - <b>Tidak memenuhi harapan pelanggan</b>
Kemungkinan	2 (Kadang kadang terjadi)
Dampak risiko	4 (Signifikan)
Besaran risiko	17
Level Risiko	<b>Tinggi</b>
Opsi penanganan risiko	Mitigasi
Rencana aksi penanganan risiko SPBE	- Evaluasi kinerja secara berkala - <b>Pelatihan dan pengembangan karyawan</b> - <b>Rekrutmen dan seleksi yang teliti</b>

Keterangan: Tulisan Bold Merupakan Hasil Rekomendasi Dari Hasil Penelitian

Pada bagian dampak penulis menambahkan tidak terpenuhinya harapan pelanggan karena dengan tidak primanya pelayanan yang diberikan dapat menyebabkan ketidakpuasan pelanggan, baik itu pihak internal dalam organisasi maupun mitra eksternal. Hal ini dapat menyebabkan kehilangan peluang kerjasama dan dukungan ke depannya.

Pada bagian rencana aksi penanganan risiko, penulis menyarankan pelatihan dan pengembangan karyawan. Program tersebut dapat dilakukan secara berkesinambungan untuk meningkatkan keterampilan dan pengetahuan personil. Ini akan membantu meningkatkan kompetensi mereka dalam memberikan layanan prima. Selain itu penulis juga menyarankan untuk melakukan rekrutmen dan seleksi yang teliti yaitu dengan memastikan proses rekrutmen dan seleksi personil dilakukan secara teliti dan obyektif sehingga hanya personil berkualitas yang diterima pada Lembaga tersebut.

TABEL V. 8

Rekomendasi personil kurang terkendali dalam mengakses aset yang sensitif

Kejadian	Personil kurang terkendali dalam mengakses aset yang sensitif
Penyebab	Tidak dipatuhinya kebijakan penggunaan dan pemanfaatan oleh pihak ke tiga
Dampak	- Keamanan SPBE tidak terjamin - <b>Pencurian data dan informasi rahasia</b>
Kemungkinan	2 (Kadang kadang terjadi)
Dampak risiko	4 (Signifikan)
Besaran risiko	17
Level Risiko	<b>Tinggi</b>
Opsi penanganan risiko	Mitigasi
Rencana aksi penanganan risiko SPBE	- Evaluasi kinerja personil pihak ke tiga secara berkala - <b>Monitoring dan audit</b> - <b>Pengaturan akses terbatas</b>

Keterangan: Tulisan Bold Merupakan Hasil Rekomendasi Dari Hasil Penelitian

Pada bagian dampak penulis menambahkan pencurian data dan informasi rahasia. Pihak ketiga yang tidak terkendali dapat menyebabkan potensi pencurian data dan informasi rahasia lembaga. Informasi tersebut dapat digunakan untuk keuntungan komersial maupun pribadi atau tujuan jahat lainnya.

Pada bagian rencana aksi penanganan risiko penulis merekomendasikan untuk melakukan *monitoring* dan *audit* secara berkala terhadap aktivitas pihak ketiga untuk memantau apakah ada upaya yang mencurigakan. Selain itu penulis juga menyarankan untuk pengaturan akses terbatas yaitu dengan cara membatasi akses pihak ketiga hanya untuk data dan informasi yang relevan dengan tugas yang diberikan. Selain itu, perlu ditentukan tingkat akses yang sesuai untuk mencegah akses tidak sah.

## VI. KESIMPULAN DAN SARAN

### A. Kesimpulan

- Dari hasil penelitian ini, implementasi manajemen risiko pada Lembaga XYZ sudah berjalan sesuai dengan pedoman dari Peraturan Menteri Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 (PERMEN PANRB) tentang pedoman manajemen risiko sistem pemerintahan berbasis elektronik. Implementasi manajemen risiko dinilai sudah sangat efektif.
- Dari hasil identifikasi dan evaluasi pada beberapa *risk register* yang telah diidentifikasi, penulis membedakan risiko tersebut menjadi 3 level risiko, yaitu sangat tinggi, tinggi, dan sedang. Pada level risiko sangat tinggi terdapat 3 risiko yaitu terjadinya kebakaran, kepemimpinan dan pengorganisasian SPBE tidak berjalan, dan aplikasi penginderaan jauh tidak dapat diakses. Lalu pada level tinggi terdapat 3 risiko yaitu keteledoran personal terhadap pengamanan data dan informasi, personil kurang mampu memberikan pelayanan risiko, personil kurang terkendali dalam mengakses aset yang

sensitif. Lalu pada level sedang terdapat 6 risiko yaitu tidak ada rekaman, sistem layanan terinfeksi virus dan/atau malware, sistem layanan mengalami gangguan / tidak dapat diakses, perangkat jaringan tidak berfungsi / terganggu, gangguan / kerusakan perangkat jaringan core Gudang, dan kabel putus

3. Rekomendasi yang penulis berikan hanya untuk level risiko sangat tinggi dan tinggi saja. Beberapa rekomendasi yang penulis tambahkan pada bagian dampak adalah seperti kehilangan data dan informasi, gangguan pada proyek penelitian, hilangnya kepercayaan masyarakat, keterbatasan pada akses informasi, dan lain-lain. Untuk rekomendasi pada bagian rencana aksi penanganan adalah seperti pemantauan keamanan, diversifikasi sumber data, pelatihan dan pengembangan karyawan, melakukan update dan patching, investasi pada infrastruktur jaringan yang handal, melakukan pemantauan secara real-time pemeliharaan perangkat secara rutin, dan lain-lain.

#### B. Saran

Berdasarkan hasil identifikasi dan evaluasi manajemen risiko PT. Xyz, terdapat beberapa saran sebagai berikut:

1. Disarankan untuk lebih melengkapi dampak dari setiap kejadian PT. Xyz, karena kemungkinan terdapat lebih dari satu dampak yang perlu dipertimbangkan.
2. Diharapkan perusahaan senantiasa melakukan evaluasi secara berkala untuk mengukur keberhasilan rencana penanganan risiko yang diambil dalam setiap risiko yang ada.

#### REFERENSI

- Hutagalung, A. (2019). Analisis Human Error Untuk Mengurangi Kecelakaan Kerja Menggunakan Metode SHERPA dan HEART (Studi Kasus di UKM Kayu Lapis CV. Cipta Mandiri Klaten). *Skripsi Teknik Industri*, 5–24.
- Jurnal, H., Majestika, A. Q., Farida, F., Ekonomi, F., Bisnis, D., & Manajemen, J. (2022). Jurnal Ilmiah Manajemen Dan Kewirausahaan Analisa Pelaksanaan Standar Operasional Prosedur (Sop) Pelayanan Oleh Staff Ticketing Di Sales Office Garuda Indonesia Senayan City. *Jimak*, 1(2).
- Meidyani Dp, W., Putu, K., Rusmala, D., Wayan, N., Restitiasih, M., Luh, N., Trisnawati, P., Tingkat, P., Kabupaten, S. P., & Abstrak, T. (2019). *Jurnal Pendidikan Fisika Mapping the Level of Lightning Strikes in Tabanan Regency*. 7, 347.
- Yonasda, C. D. P. (2020). *Analisis Quality of Service Jaringan Internet Dengan Menggunakan Aplikasi Wireshark Di Smkn 1 Mesjid Raya Ujoeng Batee*. 1–23.
- Djojosoedarso, S. 2003. Prinsip-Prinsip Manajemen Risiko dan Asuransi, Edisi. Revisi. Jakarta: Salemba Empat.
- Arthur, J. Keown dkk. 2000. Dasar-Dasar Manajemen Keuangan. Jakarta: Salemba

Empat.

- Purwanto, A. M. G., Novianti, E., & ... (2022). Proses Belajar Seorang Anak Tunarungu Melalui Pendekatan Photo Story. *Jurnal Dimensi DKV* ..., 15–34. <http://trijurnal.lemli.trisakti.ac.id/index.php/seni/articledownload/12831/7972>
- Saputro, T., & Lombardo, D. (2021). Metode Hazard Identification, Risk Assessment And Determining Control (HIRADC) Dalam Mengendalikan Risiko Di PT. Zae Elang Perkasa. *Jurnal Baut Dan Manufaktur*, 03(1), 23–29. <https://uia.e-journal.id/bautdanmanufaktur/article/download/1316/761/>
- ISACA. (2018). Introduction and methodology. In *Developing Reading and Writing in Second-Language Learners: Lessons from the Report of the National Literacy Panel on Language-Minority Children and Youth: Second Edition*. <https://doi.org/10.4324/9780203937600>
- Wardani, S., & Puspitasari, M. (2014). Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit Dengan Model Maturity Level ( Studi Kasus Fakultas Abc ). *Jurnal Teknologi*, 7(1), 38–46. <http://journal.akprind.ac.id/index.php/jurtek/article/view/516>
- Koontz, Harold, Cyrril O'Donnel, dan Heinz Weihrich. 2004. Management. Singapore: McGraw Hill.
- Sugiyono. 2016. Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta
- Parlika, R., Lintang P, H., Setia R, I., Suriansyah, M., Humania B, N., Yulianto, E., & Aulia N, R. (2018). Pengaruh mutu dan pemeliharaan perangkat lunak pada kelayakan dan hasil validasi aplikasi. *NJCA (Nusantara Journal of Computers and Its Applications)*, 3(1). <https://doi.org/10.36564/njca.v3i1.67>
- Hartanto, W. (2018). Cloud Computing Dalam Pengembangan Sistem. *Jurnal Pendidikan Ekonomi: Jurnal Ilmiah Ilmu Pendidikan, Ilmu Ekonomi Dan Ilmu Sosial*, 10(2), 1–10. <https://jurnal.unej.ac.id/index.php/JPE/article/view/3810>
- Mamduh, H. (2015). Konsep Dasar dan Perkembangan Teori Manajemen. *Manajemen*, 1(1), 7. <http://repository.ut.ac.id/4533/1/EKMA4116-M1.pdf>
- Lokobal, A., Sumajouw, M. D. J., & Sompie, B. F. (2014). Manajemen Risiko Pada Perusahaan Jasa Pelaksana Konstruksi di Propinsi Papua (Study Kasus di Kabupaten Sarmi). *Jurnal Ilmiah Media Engineering*, 4(2), 109–118.