Analisis Manajemen Risiko dengan Menggunakan Framework ISO 31000:2018 pada Sistem Informasi E-Gudang Satpol PP Kota Surabaya

Birgita Yolanda F.A.H*[1], Muhammad Nasrullah[2], Aris Kusumawati[3]
[1,2]Telkom University; Jl. Ketintang No.156, Ketintang, Kec. Gayungan, Kota Surabaya, Jawa Timur 60231, (031) 8294608 / (031) 8294517
[3]Fakultas Rekayasa Industri, Telkom University
e-mail: *[1]birgitaayf@student.telkomuniversity.ac.id, [2]emnasrul@telkomuniversity.ac.id, [3]ariskusumawati@telkomuniversity.ac.id

Abstrak

Peran teknologi dalam dunia bisnis saat ini menjadi semakin penting, khususnya dalam mendukung perkembangan perusahaan atau organisasi. Dengan mengoptimalkan Sistem Informasi/Teknologi Informasi (SI/TI), instansi dapat meningkatkan daya saing mereka. Namun, optimalisasi aset teknologi informasi juga meningkatkan risiko yang dapat mengancam pencapaian tujuan perusahaan. Manajemen risiko SI/TI yang efektif sangat penting untuk memaksimalkan kegunaan aset teknologi informasi dan meningkatkan efisiensi proses bisnis. Satuan Polisi Pamong Praja (Satpol PP) memerlukan manajemen risiko SI/TI yang baik, terutama untuk Sistem Informasi E-Gudang yang digunakan untuk mengelola Barang Hasil Penertiban (BHP). Risiko kehilangan data, kebocoran informasi, dan kesalahan input sata menjadi tantangan yang dihadapi oleh Satpol PP Kota Surabaya. Sistem Informasi E-Gudang membantu mengontrol BHP, mengelola stok, dan terintegrasi dengan bidang lain seperti bidang ketentraman dan umum. Namun, risiko yang mengancam operasional tetap ada. Oleh karena itu, diperlukan analisis manajemen risiko teknologi informasi yang komprehensif. Metode ISO 31000:2018 digunakan untuk mengidentifikasi, menilai, dan mengelola risiko-risiko tersebut. ISO 31000:2018 menyediakan panduan untuk *risk assessment*, membantu dalam melihat nilai risiko dari setiap risiko yang telah teridentifikasi. Penelitian ini bertujuan meminimalisir risiko yang mungkin terjadi dan memberikan rekomendasi bagi Satpol PP terkait risiko pada Sistem Informasi E-Gudang. Hasil dari penelitian yang telah dialkukan ini ditemukan 12 kemungkinan ancaman risiko diantaranya Terdapat 2 dengan tingkatan *high,* 9 risiko dengan tingkatan *medium* dan yang terakhir yaitu dengan 1 risiko memiliki tingkatan *low.*

Kata Kunci: Analisis Risiko, E-Gudang, ISO 31000:2018, Manajemen Risiko

Risk Management Analysis Using the ISO 31000:2018 Framework on the E-Gudang Information System of the Civil Service Police Unit of Surabaya City

Abstract

The role of technology in today's business world is becoming increasingly important, especially in supporting the growth of companies or organizations. By optimizing Information Systems/Information Technology (IS/IT), institutions can enhance their competitiveness. However, the optimization of information technology assets also increases the risk that can threaten the achievement of company goals. Effective IS/IT risk management is crucial to maximizing the usefulness of information technology assets and improving business process efficiency. The Civil Service Police Unit (Satpol PP) requires good IS/IT risk management, particularly for the E-Gudang Information System used to manage Confiscated Goods (BHP). The risks of data loss, information leakage, and data input errors are challenges faced by Satpol PP in Surabaya. The E-Gudang Information System helps control BHP, manage inventory, and is integrated with

other departments such as the public order and general affairs divisions. However, operational risks remain. Therefore, a comprehensive information technology risk management analysis is needed. The ISO 31000:2018 method is used to identify, assess, and manage these risks. ISO 31000:2018 provides guidelines for risk assessment, helping to evaluate the risk value of each identified risk. This study aims to minimize potential risks and provide recommendations to Satpol PP regarding risks in the E-Gudang Information System. The results of this study found 12 potential risk threats, including 2 with a high level, 9 with a medium level, and 1 with a low level.

Keywords: *E-Gudang, ISO 31000:2018, Risk Analysis, Risk Management*

1. Pendahuluan

Di era sekarang, teknologi merupakan elemen penting dalam bisnis dan membantu kemajuan perusahaan dan organisasi. Dengan berhasilnya pengembangan sistem informasi/teknologi informasi (SI/IT) pada suatu perusahaan atau organisasi, maka perusahaan dapat bersaing dengan para kompetitornya [1]. Namun, dengan infrastruktur TI yang lebih efektif muncul risiko lebih besar terhadap masalah yang mengganggu perusahaan dan mempersulit pencapaian tujuannya. Mengelola risiko TI/SI dalam suatu perusahaan atau organisasi dapat membuat aset TI menjadi lebih efisien dan meningkatkan efisiensi dan efektivitas operasional bisnis. Bisnis yang sukses memahami pentingnya mengelola risiko yang terkait dengan perencanaan dan/atau implementasi TI. Manajemen risiko SI/TI penting tidak hanya untuk satu sektor, namun juga untuk berbagai sektor industri, termasuk sektor publik dan layanan publik.[2].

Satuan Polisi Pamong Praja (Satpol PP) sebagai bagian dari instansi pemerintah juga memerlukan manajemen risiko SI/TI yang baik. Sistem Informasi E-Gudang yang digunakan oleh Satpol PP untuk mengelola Barang Hasil Penertiban (BHP) mereka adalah salah satu contoh penting aplikasi SI/TI yang harus dikelola dengan baik untuk menghindari risiko yang dapat mengganggu operasional dan layanan publik [3]. Namun, seiring dengan penerapan teknologi informasi, muncul pula berbagai risiko yang dapat mengancam keamanan dan integritas data yang tersimpan di Sistem Informasi e-Gudang. Risiko kehilangan data, kebocoran informasi, dan kesalahan input data menjadi tantangan yang harus dihadapi [4]. Selain itu masalah lain yang dialami oleh Satpol PP Kota Surabaya itu masih adanya beberapa proses yang menggunakan cara manual pada proses pencatatan BHP nya, data tidak terpantau dengan baik, dan lain sebagainya.

Sistem Informasi E-Gudang di Satpol PP membantu mengontrol BHP yang masuk dan keluar, mengelola stok BHP, serta terintegrasi dengan bidang lain seperti bidang Ketentraman dan Penertiban Umum. Namun tidak dapat dipungkiri bahwa masih terdapat kemungkinan sistem informasi elektronik dapat mengancam dan mengganggu proses bisnis. Oleh karena itu, analisis manajemen risiko TI yang komprehensif diperlukan untuk mengidentifikasi, menilai, dan mengelola risiko-risiko tersebut [2]. Manajemen risiko yang baik menggunakan metode ISO 31000:2018 sangat diperlukan untuk mengelola risiko aset SI/TI di Satpol PP. ISO 31000:2018 merupakan panduan dasar bagi manajemen untuk menetapkan kerangka manajemen risiko yang mencakup perencanaan, akuntabilitas personel, aset, dan aktivitas yang terlibat dalam manajemen risiko [5]. Dengan menerapkan rencana penilaian, analisis, dan mitigasi risiko berdasarkan standar ISO 31000:2018, diharapkan risiko yang mungkin terjadi dapat dikurangi [6].

Tujuan dari penelitian ini adalah untuk meminimalisir segala permasalahan yang mungkin terjadi dan memberikan saran yang tepat kepada Satpol PP mengenai permasalahan yang mungkin timbul pada sistem komunikasi elektronik. Analisis risiko ini dilakukan dengan menggunakan metodologi ISO 31000:2018. ISO 31000:2018 memberikan pedoman untuk melakukan penilaian risiko untuk membantu menentukan nilai risiko dari suatu bahaya yang teridentifikasi. Oleh karena itu, penelitian ini diharapkan dapat memberikan kontribusi terhadap manajemen risiko SI/TI di Satpol PP dan berkontribusi terhadap peningkatan efisiensi dan efektivitas operasional melalui manajemen risiko yang baik.

2. Metode Penelitian

2.1 Penelitian Sebelumnya

Pada penelitian dengan judul Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018 [7] membahas mengenai implementasi kerangka kerja ISO 31000:2018 pada unit di instansi perguruan tinggi untuk memahami risiko yang dapat mempengaruhi proses bisnis BTSI. Memaparkan pandangan dari risiko yang mengintai dan menjadi ancaman terkait teknologi informasi pada organisasi serta berdampak buruk pada pihak stakeholder/vendor organisasi, sehingga dapat memitigasi risiko yang mungkin dapat terjadi merupakan manfaat penerapan audit manajemen risiko.

Penelitian selanjutnya dengan judul Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang [8] dengan memitigasi segala permasalahan yang mungkin terjadi atau tidak, serta dengan menyediakan materi CV dan nasehat yang tepat untuk setiap permasalahan yang mungkin timbul sewaktu-waktu. Analisis risiko ini dilakukan dengan menggunakan metodologi ISO 31000:2018.

Terakhir penelitian yang berjudul Manajemen Risiko Teknologi Informasi Aplikasi E-Office ASN Menggunakan ISO 31000:2018 [4] untuk menerapkan manajemen risiko TI dengan menggunakan standar ISO 31000:2018 dalam pengelolaan dan pemeliharaan aplikasi E-Office ASN yang digunakan oleh ASN (Pegawai Negeri Sipil) di Kabupaten Sumedang. Tujuan-tujuan ini ditentukan dalam beberapa tahap. Pertama, tujuan penelitian ini adalah untuk mengidentifikasi secara akurat risiko-risiko yang terjadi pada penggunaan aplikasi ASN E-Office oleh Pegawai Negeri Sipil (PNS) dan PPPK (pegawai pemerintah dan kontrak kerja) di wilayah Sumedang. Tujuan dari penelitian ini adalah untuk mengetahui tingkat risiko untuk setiap risiko yang teridentifikasi berdasarkan kriteria yang relevan dan mengacu pada standar ISO 31000:2018.

2.2 Landasan Teori

2.2.1 Pengertian Satuan Polisi Pamong Praja

Menurut Undang-Undang Pemerintah Republik Indonesia Nomor 16 Pasal 1 Tahun 2018, Kepolisian Daerah (Satpol PP) adalah badan daerah yang dibentuk untuk melaksanakan peraturan daerah dan peraturan kepala daerah [9]. Tugasnya adalah mengatur kehidupan masyarakat, perdamaian dan melindungi masyarakat. Polisi Pamong Praja atau Pol PP adalah anggota Satpol PP dan merupakan pegawai negeri sipil. Mereka mempunyai tugas, tanggung jawab, dan wewenang yang ditetapkan dengan undang-undang dalam melaksanakan peraturan daerah dan peraturan daerah, serta bertugas memelihara ketertiban umum, ketentraman, dan perlindungan masyarakat [10].

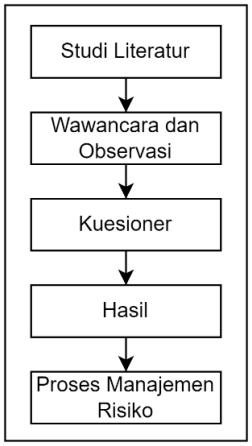
2.2.2 Pengertian Manajemen Risiko

Manajemen risiko adalah proses sistematis untuk mengidentifikasi, menilai dan mengendalikan risiko yang mungkin mempengaruhi pencapaian tujuan organisasi. Dalam konteks TI, manajemen risiko melibatkan identifikasi ancaman terhadap sistem informasi, menilai kerentanan, dan menerapkan pengendalian untuk mengurangi dampak risiko tersebut [11].

2.3 Metodologi Penelitian

2.3.1 Metode Pengumpulan Data

Penelitian ini dilakukan dengan pendekatan kuantitatif, pengumpulan datanya meliputi informasi yang mencakup permasalahan, kajian dan permasalahan yang disesuaikan dengan situasi, kondisi dan fakta pada sistem informasi Satpol PP Kota Surabaya. Hasil penelitian ini akan digunakan sebagai dasar evaluasi atau perbaikan sistem informasi elektronik Satpol PP Kota Surabaya.

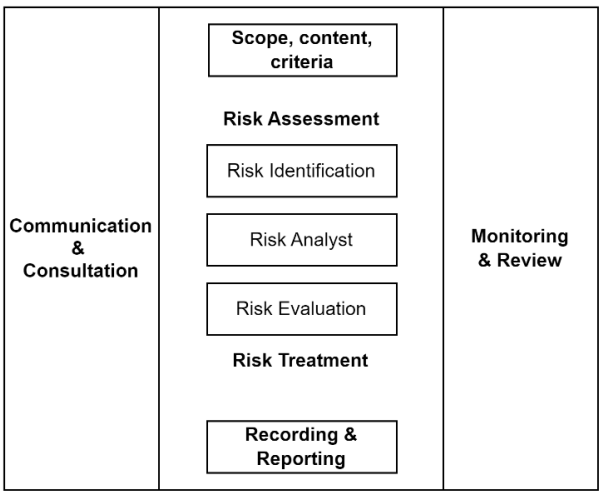


Gambar 1. Tahapan Pengumpulan Data

Metode pengumpulan data yang digunakan adalah penelitian kepustakaan yaitu tinjauan literatur dan teori terkait yang dijadikan acuan dalam penelitian ini. Selain itu observasi dilakukan dengan melihat secara langsung apa yang telah dipelajari. Metode pengumpulan data terakhir adalah kuesioner yang pertanyaannya dikirimkan kepada responden dengan menggunakan sistem informasi e-Gudang. Pada langkah terakhir, proses manajemen risiko dijelaskan pada bagian analisis data.

2.4 Metode Analisis Data

Analisis data adalah proses sistematis pengumpulan dan pencarian data, mulai dari identifikasi masalah hingga pengambilan keputusan. Proses ini didasarkan pada data yang diperoleh dari berbagai metode pengumpulan data seperti penelitian literatur, wawancara, observasi dan angket. Dalam penelitian ini metode analisis data yang digunakan adalah framework ISO 31000:2018 yang bertujuan untuk mengidentifikasi potensi ancaman yang mungkin terjadi pada sistem informasi elektronik Satpol PP Surabaya [12]. ISO 31000:2018 adalah standar manajemen risiko yang diterbitkan oleh Organisasi Internasional untuk Standardisasi pada 13 November 2009. Standar ini dirancang untuk digunakan dan diadaptasi oleh berbagai jenis organisasi dan memberikan kerangka kerja serta panduan umum untuk semua aktivitas yang terkait dengan manajemen risiko [13]. Tahapan-tahapan dalam metode penelitian yang digunakan dalam penyusunan paper ini dapat dilihat pada Gambar 2.



Gambar 2. Proses *Risk Management ISO 31000:2018*

Gambar 2 merupakan proses manajemen risiko menggunakan ISO 31000:2018 yang terdiri dari:

a) *Communication dan Concultation*
b) *Scope, content, and Criteria*
c) *Risk assessment*
d) *Risk Treatment*
e) *Monitoring and Review*

Setelah menyelesaikan berbagai tahapan manajemen risiko yang telah disebutkan, peneliti akan menetapkan tingkat risiko untuk setiap risiko yang ada di area penelitian.

2.5 Rumus yang digunakan

Untuk menghitung hasil kuesioner, peneliti menggunakan model Likert. Untuk mengetahui persentase tanggapan masing-masing responden digunakan skala likert dan rumus sebagai berikut [14]:

$$\text{Rata} - \text{rata peluang} = \frac{\sum_1^n Peluang}{Jumlah\ responden\ (n)}\ x\ 100 \qquad (1)$$

$$\text{Rata} - \text{rata dampak} = \frac{\sum_1^n Dampak}{Jumlah\ responden\ (n)}\ x\ 100 \qquad (2)$$

$$\text{Risiko} = \frac{\sum_1^n PeluangxDampak}{Jumlah\ responden\ (n)} \qquad (3)$$

Hasil dari rata-rata peluang dan rata-rata dampak nantinya dibulatkan untuk memudahkan dalam perhitungan indeks risiko.

3. Hasil Penelitian

Hasil penelitian merupakan hasil rumusan masalah dan penggunaan metodologi penelitian. Diharapkan metode dan teknik analisis data serta metode yang digunakan dalam proyek penelitian dapat menjawab permasalahan yang diajukan, mencapai solusi dan. gunakan sebagai referensi. Otoritas Pengembangan Organisasi.

3.1 Framework Risk Management ISO 31000

Kerangka kerja merupakan pengaturan sistem manajemen risiko yang dirancang secara terstruktur dan sistematis di seluruh organisasi.

3.1.1 Leadership and Commitment

Kepala Satpol PP Kota Surabaya memegang tanggung jawab utama dalam mengelola dan mengawasi manajemen risiko di lingkungan Satpol PP. Dalam hal ini, kepala Satpol PP harus memastikan bahwa manajemen risiko terintegrasi ke dalam semua kegiatan dan fungsi organisasi. Komitmen dari pimpinan sangat penting untuk memastikan bahwa proses manajemen risiko berjalan dengan efektif dan bahwa semua anggota tim memahami pentingnya manajemen risiko dalam operasi sehari-hari. Kepemimpinan yang kuat juga diperlukan untuk menetapkan prioritas dan alokasi sumber daya yang tepat dalam proses manajemen risiko.

3.1.2 Integration

Integrasi manajemen risiko ke dalam struktur organisasi Satpol PP Kota Surabaya dilakukan dengan memahami konteks internal dan eksternal yang memengaruhi organisasi. Ini termasuk struktur organisasi, lingkungan operasional, dan faktor-faktor lain yang memengaruhi risiko.

3.1.3 Design

Proses perancangan kerangka kerja manajemen risiko di Satpol PP Kota Surabaya melibatkan penentuan metodologi, alat, dan pendekatan yang akan digunakan untuk mengelola risiko. Kerangka kerja

ini dirancang dengan mempertimbangkan tujuan organisasi, serta memastikan bahwa proses manajemen risiko dapat diintegrasikan ke dalam setiap kegiatan operasional.

3.1.4 Implementation

Pada tahap implementasi, Satpol PP Kota Surabaya menerapkan kerangka kerja manajemen risiko dengan mengalokasikan sumber daya yang diperlukan, termasuk personel yang kompeten, teknologi, dan prosedur yang sesuai. Proses ini mencakup pengembangan rencana implementasi yang detail, serta identifikasi area di mana keputusan terkait risiko harus dibuat. Implementasi ini juga melibatkan komunikasi yang efektif dengan semua pihak terkait untuk memastikan pemahaman yang konsisten mengenai risiko dan langkah-langkah penanganannya.

3.1.5 Evaluation

Setelah kerangka kerja manajemen risiko diterapkan, Satpol PP harus melakukan evaluasi berkala terhadap efektivitasnya. Evaluasi ini bertujuan untuk mengukur kinerja kerangka kerja terhadap tujuan yang telah ditetapkan dan untuk menentukan apakah kerangka kerja tersebut tetap relevan dan efektif dalam mendukung pencapaian tujuan organisasi. Evaluasi juga membantu dalam mengidentifikasi area yang memerlukan perbaikan atau penyesuaian lebih lanjut.

3.1.6 Improvement

Proses perbaikan dalam kerangka kerja manajemen risiko ISO 31000 melibatkan pemantauan terus-menerus terhadap efektivitas kerangka kerja dan adaptasi terhadap perubahan yang terjadi baik secara internal maupun eksternal. Satpol PP Kota Surabaya harus siap untuk melakukan penyesuaian yang diperlukan untuk meningkatkan kesesuaian, kecukupan, dan efektivitas kerangka kerja manajemen risiko. Perbaikan ini melibatkan pengembangan rencana tindakan untuk mengatasi celah atau peluang yang diidentifikasi selama evaluasi, serta memastikan bahwa perbaikan yang dilakukan dapat memberikan nilai tambah bagi organisasi.

3.2 Process Risk Management ISO 31000

Pada tahapan ini akan dijelaskan beberapa langkah utama yang dirancang untuk membantu organisasi dalam mengidentifikasi, menilai, dan mengelola risiko secara efektif. Berikut adalah langkah-langkahnya:

3.2.1 Communication and Consultation

Pada tahap ini, peneliti mengajukan hasil kegiatan magang terkait manajemen risiko teknologi informasi kepada instansi Satuan Polisi Pamong Praja Kota Surabaya, yang merupakan tempat magang peneliti. Selanjutnya, peneliti mengadakan diskusi dan wawancara dengan staf bagian informatika.

3.2.2 Scope, Content and Criteria

Pada langkah ini peneliti menganalisis manajemen risiko TI di Satuan Polisi Pamong Praja Kota Surabaya, terhadap tujuan penelitian E-Gudang, sistem informasi yang dikelola Satpol PP Kota Surabaya, dan berdasarkan laporan pengguna. Atau seorang manajer yang sistem informasinya memiliki risiko tinggi kehilangan data dan kesalahan entri data [15]. Risiko yang dianalisis adalah risiko yang berkaitan dengan penggunaan E-Gudang. Adapun konteks E-Gudang adalah sebagai berikut:

A. Sumber Daya Manusia (User)
B. Sistem dan Infrastruktur
C. Pelaporan

3.2.3 Risk Assessment

Penilaian risiko adalah proses yang mencakup identifikasi, analisis, dan evaluasi risiko. Proses ini dilakukan secara sistematis, berulang, dan melibatkan kerja sama antara berbagai pemangku kepentingan. Penilaian ini didasarkan pada pengetahuan serta perspektif para pemangku kepentingan terkait risiko yang dihadapi. Dengan melibatkan pemangku kepentingan, penilaian risiko menjadi lebih komprehensif, karena

memanfaatkan wawasan yang berbeda untuk mengidentifikasi potensi ancaman dan dampaknya secara lebih akurat [16].

A. *Risk Identification*

Tahap identifikasi risiko bertujuan untuk mengungkap berbagai potensi risiko yang mungkin timbul. Proses ini dilakukan setelah melalui studi literatur dan wawancara dengan pihak-pihak terkait dengan Sistem Informasi E-Gudang, yaitu para pemangku kepentingan dan bidang informatika Satpol PP Kota Surabaya. Pada tahap ini, informasi dikumpulkan untuk mengidentifikasi risiko-risiko yang berpotensi muncul dalam proses bisnis instansi [16].

Proses identifikasi ini mengikuti pedoman dari konteks yang telah disetujui sebelumnya dalam tahap penetapan konteks. Pada tahap penetapan konteks, telah ditentukan tiga aspek utama yang menjadi batasan atau tolak ukur, baik internal maupun eksternal, yang digunakan untuk mempertimbangkan sumber-sumber risiko, yaitu: Sumber Daya Manusia (User), Sistem dan Infrastruktur serta Pelaporan .

- Identifikasi Aset

  Pada tahap ini akan dilakukan identifikasi aset yang dihasilkan dari proses observasi pada Sistem Informasi E-Gudang, identifikasi ini melibatkan aset yang dimiliki seperti data, *software,* serta *hardware* yang terdapat pada Sistem Informasi E-Gudang.

Tabel 1 Identifikasi Aset pada Sistem Informasi E-Gudang Satpol PP Kota Surabaya

Komponen SI/TI	Aset pada Sistem Informasi E-Gudang Satpol PP Kota Surabaya
Data	1. Data Barang Hasil Penertiban Masuk 2. Data Barang Hasil Penertiban Keluar
Software	Sistem Informasi E-Gudang (Sistem Informasi penyimpanan data Barang Hasil Penertiban) Gudang Tanjungsari dan Mako Satuan Polisi Pamong Praja Kota Surabaya
Hadware	Device (PC)

- Identifikasi Kemungkinan Risiko

  Setelah mengidentifikasi aset dalam Sistem Informasi E-Gudang, langkah berikutnya adalah mengidentifikasi kemungkinan risiko yang mungkin timbul. Risiko-risiko ini dapat berasal dari berbagai faktor, termasuk Sumber Daya Manusia (User), sistem dan infrastruktur serta Pelaporan yang terkait dengan penggunaan E-Gudang.

Tabel 2 Identifikasi Kemungkinan Risiko

Kategori Risiko	Id	Risiko	Penyebab
Sumber Daya Manusia (User)	R1	Kesalahan input data	Kurangnya pelatihan atau pemahaman pengguna tentang cara memasukkan data dengan benar, atau antarmuka pengguna yang membingungkan.
	R2	User tidak dilatih dengan baik	Program pelatihan yang tidak memadai atau tidak ada sama sekali, kurangnya pendampingan atau panduan dalam penggunaan sistem.
	R3	Kehilangan database	Pengawasan yang kurang, prosedur penanganan barang yang tidak jelas, atau tidak adanya sistem tracking yang efektif.
Sistem dan Infrastruktur	R4	Database barang masuk tidak terupdate	Proses update data yang manual dan rentan terhadap kesalahan, tidak adanya prosedur otomatisasi dalam pembaruan data stok.
	R5	Kebocoran data sensitif	Keamanan sistem yang tidak memadai, akses yang tidak terbatas pada data sensitif, atau kelemahan dalam protokol keamanan.
	R6	Gagal melakukan backup data	Tidak adanya prosedur backup yang rutin, kelalaian dalam menjalankan prosedur backup, atau masalah teknis pada sistem backup.
	R7	Akses tidak sah oleh user	Sistem keamanan yang lemah, kata sandi yang mudah ditebak, atau tidak adanya autentikasi dua faktor.

	R8	Gangguan operasional saat update	Kurangnya perencanaan dalam jadwal pembaruan, atau pembaruan dilakukan tanpa menguji dampaknya terlebih dahulu.
	R9	Data yang tersimpan tidak sinkron	Integrasi yang buruk antara sistem yang berbeda, atau sistem yang usang dan tidak mendukung fitur baru.
	R10	Maintenance yang lama	Ketersediaan sumber daya teknis yang terbatas, atau tidak adanya prosedur tanggap darurat yang efektif.
	R11	Terjadinya data duplicate	Prosedur input data yang tidak jelas, atau kurangnya sistem deteksi duplikasi.
Pelaporan	R12	Output download yang tidak sesuai	Kesalahan dalam pengumpulan atau analisis data, atau tidak adanya sistem verifikasi dan validasi data sebelum laporan dibuat.

- Identifikasi Dampak Risiko

Setelah tahap identifikasi risiko dilakukan, beberapa risiko potensial terdeteksi dari berbagai faktor seperti Sumber Daya Manusia (User), sistem dan infrastruktur serta Pelaporan yang dapat mengancam kinerja Sistem Informasi E-Gudang. Oleh karena itu, analisis terhadap dampak yang ditimbulkan oleh risiko-risiko ini perlu dilakukan.

Tabel 3 Identifikasi Dampak Risiko

Id	Kemungkinan Risiko	Dampak
R1	Kesalahan input data	Kesalahan dalam pengambilan dan kehilangan kepercayaan.
R2	User tidak dilatih dengan baik	Penggunaan sistem yang tidak efisien, kesalahan operasional, dan penurunan produktivitas.
R3	Kehilangan database	Penggunaan sistem yang tidak efisien, kesalahan operasional, dan penurunan produktivitas.
R4	Database barang masuk tidak terupdate	Terganggunya operasional dan tidakjelasan data
R5	Kebocoran data sensitif	Pelanggaran privasi, kerugian reputasi, dan potensi tuntutan hukum.
R6	Gagal melakukan backup data	Kehilangan data penting, gangguan operasional, dan biaya pemulihan data yang tinggi.
R7	Akses tidak sah oleh user	Potensi manipulasi data, kebocoran informasi, dan risiko keamanan.
R8	Gangguan operasional saat update	Terhentinya proses bisnis, kehilangan pendapatan, dan gangguan pelayanan kepada pelanggan.
R9	Data yang tersimpan tidak sinkron	Inefisiensi operasional, peningkatan biaya perbaikan, dan gangguan integrasi antar sistem.
R10	Maintenance yang lama	Downtime yang lama, penurunan produktivitas, dan potensi kehilangan pelanggan.
R11	Terjadinya data duplicate	Kebingungan dalam pengambilan keputusan, kesalahan laporan, dan peningkatan waktu analisis.
R12	Output download yang tidak sesuai	Keputusan bisnis yang salah, kerugian finansial, dan kehilangan kepercayaan dari pemangku kepentingan.

B. *Risk Analyst*

Pada tahap ini, dilakukan analisis risiko dengan menilai kemungkinan-kemungkinan risiko yang telah diidentifikasi sebelumnya. Dalam menilai kemungkinan risiko, dilakukan pemberian skor pada frekuensi dari setiap kemungkinan risiko, dengan nilai berkisar dari 1 hingga 5. Nilai ini ditentukan berdasarkan tingkat frekuensi kejadian dan dampak dari risiko tersebut. Semakin tinggi nilai yang diberikan, semakin sering risiko tersebut terjadi atau semakin besar dampaknya. Tabel 2 dan Tabel 3 di bawah ini menunjukkan tabel frekuensi kemungkinan kejadian dan penilaian dampak risiko secara lebih rinci.

Tabel 4 Kriteria *Likelihood*

Kriteria	Keterangan	Nilai	Frekuensi Kejadian
Certain	Risiko hampir selalu terjadi	5	< 7 bulan
Likely	Risiko sering terjadi	4	7 – 12 bulan
Possible	Risiko kadang terjadi	3	1 – 3 tahun
Unlike	Risiko jarang terjadi	2	3 – 5 tahun
Rare	Risiko hampir tidak pernah terjadi	1	> 5 tahun

Tabel 5 Kriteria *Impact*

Kriteria	Nilai	Keterangan
Major	5	Risiko tidak menganggu aktivitas dan proses bisnis pada instansi
High	4	Gangguan signifikan, seperti penurunan kinerja atau kehilangan akses sementara.
Moderate	3	Gangguan moderat, seperti keterlambatan atau penurunan kualitas layanan.
Minor	2	Dampak kecil yang tidak mempengaruhi operasional secara keseluruhan.
Insignificant	1	Dampak sangat rendah atau tidak ada dampak nyata. Tidak memerlukan tindakan.

Berdasarkan kriteria *Likelihood* pada Tabel 4 dan kriteria *Impact* pada Tabel 5, langkah berikutnya adalah melakukan penilaian kemungkinan risiko dengan merujuk pada tabel-tabel tersebut.

Tabel 6 Penilaian *Likelihood* dan *Impact*

Id	Kemungkinan Risiko	*Likelihood*	*Impact*
R1	Kesalahan input data	3	2
R2	User tidak dilatih dengan baik	2	4
R3	Kehilangan database	4	1
R4	Database barang masuk tidak terupdate	4	3
R5	Kebocoran data sensitif	2	3
R6	Gagal melakukan backup data	4	4
R7	Akses tidak sah oleh user	2	1
R8	Gangguan operasional saat update	4	4
R9	Data yang tersimpan tidak sinkron	4	2
R10	Maintenance yang lama	4	1
R11	Terjadinya data duplicate	3	4
R12	Output download yang tidak sesuai	3	4

Dari hasil Tabel 6, diperoleh nilai-nilai kemungkinan dan dampak dari risiko-risiko yang telah teridentifikasi. Setelah itu, nilai *Likelihood* dan Impact dihitung, yang kemudian digunakan untuk melakukan evaluasi risiko.

C. *Risk Evaluation*

Tahap akhir dalam proses manajemen risiko pada penelitian ini adalah evaluasi risiko, di mana dilakukan penilaian terhadap semua potensi risiko yang telah dianalisis pada tahap sebelumnya. Proses ini menghasilkan penilaian risiko yang dikategorikan ke dalam tiga tingkat, yaitu: *Low*, *Medium*, dan *High*.

Tabel 7 Matrix Evaluasi Risiko

Likelihood	*Certain*	5	*Medium*	*Medium*	*High*	*High*	*High*
	Likely	4	*Medium*	*Medium*	*Medium*	*High*	*High*
	Possible	3	*Low*	*Medium*	*Medium*	*Medium*	*High*
	Unlikely	2	*Low*	*Low*	*Medium*	*Medium*	*Medium*
	Rare	1	*Low*	*Low*	*Low*	*Medium*	*Medium*
	Impact		1	2	3	4	5
			Insigficant	*Minor*	*Moderate*	*Major*	*Catastrop*

Sumber: [16]

Pengklasifikasian rasio berdasarkan tingkat risiko dilakukan secara berurutan dari tinggi ke rendah seperti terlihat pada Tabel 7. Setiap Id risiko yang teridentifikasi kemudian akan ditempatkan dalam matriks evaluasi risiko, dengan mengacu pada kriteria *Likelihood* dan *Impact*.

Tabel 8 Matrix Evaluasi Risiko berdasarkan *Likelihood* dan *Impact*

Likelihood	*Certain*	5					
	Likely	4	R3, R10	R9	R4	R6, R8	
	Possible	3		R1		R11, R12	
	Unlikely	2	R7		R5	R2	
	Rare	1					
	Impact		1	2	3	4	5
			Insigficant	*Minor*	*Moderate*	*Major*	*Catastrop*

Dalam proses manajemen risiko, Tabel 8 digunakan untuk menunjukkan bagaimana risiko diukur berdasarkan kemungkinan terjadinya dan dampaknya. Setelah mengidentifikasi 12 kemungkinan risiko, langkah selanjutnya adalah mengkategorikan risiko tersebut berdasarkan kriteria yang telah ditetapkan. Klasifikasi ini penting dalam menentukan jumlah perhatian dan tindakan yang diperlukan untuk setiap bahaya. Dengan cara ini, risiko dapat diklasifikasi menjadi tingkat rendah, sedang, dan tinggi, yang berkontribusi terhadap pengorganisasian organisasi dan alokasi sumber daya.

Tabel 9 Pengelompokkan Risiko berdasarkan Tingkatan

Id	Kemungkinan Risiko	*Likelihood*	*Impact*	L X I	*Risk Level*
R1	Kesalahan input data	3	2	6	*Medium*
R2	User tidak dilatih dengan baik	2	4	8	*Medium*
R3	Kehilangan database	4	1	4	*Medium*
R4	Database barang masuk tidak terupdate	4	3	12	*Medium*
R5	Kebocoran data sensitif	2	3	6	*Medium*
R6	Gagal melakukan backup data	4	4	16	*High*
R7	Akses tidak sah oleh user	2	1	2	*Low*
R8	Gangguan operasional saat update	4	4	16	*High*
R9	Data yang tersimpan tidak sinkron	4	2	8	*Medium*
R10	Maintenance yang lama	4	1	4	*Medium*
R11	Terjadinya data duplicate	3	4	12	*Medium*
R12	Output download yang tidak sesuai	3	4	12	*Medium*

Tabel 9 ini menggambarkan serangkaian 12 penilaian risiko di mana faktor-faktor risiko yang dicurigai dianalisis dan diklasifikasikan menurut tingkat risiko. Ada 2 level atas, R6 dan R8. Lalu ada 9 risiko tingkat menengah yaitu R1, R2, R3, R4, R5, R9, R10, R11 dan R12. Jadi yang terakhir mempunyai 1 peluang yaitu level rendah R7.

3.2.4 Risk Treatment

Setelah menyelesaikan analisis risiko, langkah berikutnya adalah tahap Perlakuan Risiko. Pada tahap ini, akan diberikan usulan tindakan untuk menangani risiko yang telah dikelompokkan sesuai dengan level risikonya berdasarkan Tabel 9.

Tabel 10 Usulan *Risk Treatment*

Id	Kemungkinan Risiko	*Risk Level*	*Risk Treatment*
R6	Gagal melakukan backup data	*High*	1. Terapkan sistem backup otomatis. 2. Uji secara berkala keandalan backup yang telah dilakukan. 3. Pertimbangkan penyimpanan backup di lokasi berbeda.
R8	Gangguan operasional saat update	*High*	1. Lakukan pembaruan sistem pada jam-jam tidak sibuk. 2. Buat rencana cadangan jika terjadi kegagalan saat pembaruan.
R1	Kesalahan input data	*Medium*	1. Terapkan pengecekan validasi data secara otomatis. 2. Lakukan pelatihan rutin untuk staf entri data.
R2	User tidak dilatih dengan baik	*Medium*	1. Adakan sesi pelatihan secara berkala. 2. Sediakan panduan penggunaan untuk pengguna.
R3	Kehilangan database	*Medium*	1. Terapkan sistem pelacakan barang.

			2. Gunakan pengemasan yang kuat dan asuransikan barang yang berharga.
R4	Database barang masuk tidak terupdate	*Medium*	1. Terapkan sistem pembaruan data secara otomatis. 2. Lakukan audit stok secara berkala untuk memastikan data *up to date*.
R5	Kebocoran data sensitif	*Medium*	1. Tingkatkan pengamanan data dengan enkripsi. 2. Lakukan pelatihan keamanan data kepada staf. 3. Implementasi kontrol akses yang lebih ketat.
R9	Data yang tersimpan tidak sinkron	*Medium*	1. Pastikan pengujian sistem kompatibilitas sebelum implementasi. 2. Gunakan protokol dan sistem standar.
R10	Maintenance yang lama	*Medium*	1. Sediakan tim support yang responsif. 2. Simpan cadangan suku cadang yang sering diperlukan untuk mempercepat perbaikan.
R11	Terjadinya data duplicate	*Medium*	1. Implementasikan alat deduplikasi data. 2. Lakukan audit data secara berkala untuk mengidentifikasi dan menghapus duplikasi.
R12	Output download yang tidak sesuai	*Medium*	1. Terapkan proses validasi data sebelum laporan dihasilkan. 2. Lakukan audit laporan secara berkala untuk memastikan keakuratan data.
R7	Akses tidak sah oleh user	*Low*	1. Terapkan autentikasi multi-faktor. 2. Monitor aktivitas login pengguna secara berkala untuk mendeteksi akses tidak sah.

Dalam tabel Tabel 10 merupakan usulan *risk treatment* dengan harapan dapat meminimalisir potensi risiko yang mungkin terjadi pada Sistem Informasi E-Gudang milik Sekretariat Satpol PP Kota Surabaya.

3.2.5 Recording and Reporting

Pendaftaran dan pelaporan dilakukan setelah penerapan langkah-langkah pengurangan risiko, kritik dan saran untuk perbaikan sistem komunikasi elektronik diberikan. Hasil penerapan manajemen risiko ini dipantau oleh dinas terkait Satpol PP Kota Surabaya. Seluruh pekerjaan yang dilakukan peneliti dilakukan oleh seluruh pekerja yang terhubung dengan pengoperasian sistem informasi elektronik tersebut.Laporan yang telah didaftarkan akan dikirimkan ke Satpol PP, dimana pemeriksa informasi dan laporan risiko dapat mengganggu proses informasi buku elektronik. Selain itu, rekomendasi diberikan untuk mengurangi risiko bagi pengelolaan di masa depan.

4. Kesimpulan dan Saran

4.1 Kesimpulan

Dari penelitian dengan judul Analisis Manajemen Risiko dengan menggunakan Framework ISO 31000:2018 pada Sistem Informasi E-Gudang Satpol PP Kota Surabaya, ditemukan bahwa terdapat 12 risiko yang dapat menghambat operasional website E-Gudang. Di antaranya, terdapat 2 risiko dengan tingkat *High*, yaitu Gagal melakukan backup data dan Gangguan operasional saat update. Selain itu, terdapat 9 risiko dengan tingkat *Medium*, seperti Kesalahan input data, User tidak dilatih dengan baik, Kehilangan database, Database barang masuk tidak terupdate. Kebocoran data sensitif, Data yang tersimpan tidak sinkron, Maintenance yang lama, Terjadinya data duplicate dan Output download yang tidak sesuai. Terdapat pula 1 risiko dengan tingkat *Low*, yaitu akses tidak sah oleh user.

Penelitian ini diharapkan dapat menjadi pedoman bagi Satpol PP Kota Surabaya dalam meminimalkan risiko-risiko tersebut melalui penerapan perlakuan risiko yang tepat, seperti menerapkan sistem backup otomatis, melakukan uji berkala terhadap keandalan backup, mempertimbangkan penyimpanan backup di lokasi berbeda, melakukan pembaruan sistem pada jam-jam tidak sibuk, dan menyusun rencana cadangan jika terjadi kegagalan saat pembaruan.

4.2 Saran

Peneliti telah menyelesaikan proses Manajemen Risiko dengan mengikuti standar ISO 31000:2018, yang dengan berdiskusi staf IT Satpol PP Kota Surabaya untuk memastikan kelancaran proses tersebut. Meskipun begitu, peneliti menyadari masih adanya beberapa kekurangan dan memberikan beberapa saran sebagai berikut:

1. Disarankan agar manajemen risiko juga diimplementasikan pada beberapa bagian lain di Satuan Polisi Pamong Praja Kota Surabaya, terutama karena masih ada beberapa teknologi informasi yang belum dilakukan manajemen risiko. Hal ini akan membantu meningkatkan kualitas organisasi secara keseluruhan.
2. Dalam menetapkan kriteria konteks, sebaiknya dilakukan analisis menyeluruh yang mencakup aspek eksternal dan internal untuk memahami sejauh mana kontribusi para pemangku kepentingan dalam operasional Sistem Informasi E-Gudang.

5. Daftar Pustaka

[1] T. Widy Chrisanty and J. Tambotoh, "ANALISIS MANAJEMEN RISIKO SISTEM INFORMASI MENGGUNAKAN ISO 31000:2018 di PT. XYZ," 2023.

[2] V. Patrick, P. Wijaya, and A. D. Manuputty, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," vol. 9, no. 2, pp. 1295–1307, 2022.

[3] N. N. Setyaningrum and E. Maria, "PENERAPAN ISO 31000:2018 UNTUK MANAJEMEN RISIKO PADA SISTEM INFORMASI SEKOLAH TERPADU," 2024.

[4] F. Mahardika, M. Agreindra H, S. A. Fatimah, and L. T. Nur F, "Manajemen Risiko Teknologi Informasi Aplikasi E-Office ASN Menggunakan ISO 31000:2018," *Infotekmesin*, vol. 14, no. 2, pp. 237–243, Jul. 2023, doi: 10.35970/infotekmesin.v14i2.1877.

[5] ISO, "ISO 31000:2018 Risk management — Guidelines," www.iso.org. Accessed: Jul. 26, 2024. [Online]. Available: https://www.iso.org/standard/65694.html

[6] Y. Erlika *et al.*, "Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000".

[7] V. Patrick, P. Wijaya, and A. D. Manuputty, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," vol. 9, no. 2, pp. 1295–1307, 2022.

[8] W. Harefa and K. D. Hartomo, "Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, pp. 407–420, Mar. 2022, [Online]. Available: http://jurnal.mdp.ac.id

[9] Peraturan Pemerintah RI, "PERATURAN PEMERINTAH REPUBLIK INDONESIA NOMOR 16 TAHUN 2018." Accessed: Aug. 15, 2024. [Online]. Available: https://peraturan.bpk.go.id/Details/77284/pp-no-16-tahun-2018

[10] H. Bahalwan, R. Puspitasari, and F. Wahmuda, "Redesain Rompi Multifungsi Satuan Polisi Pamong Praja (Satpol PP)," *Jurnal Ilmu Komputer dan Desain Komunikasi Visual*, vol. 9, no. 1, Jul. 2024.

[11] G. Stoneburner, A. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*. Gaithersburg: National Institute of Standards and Technology Special Publication, 2002.

[12] R. I. Liperda and U. Ayu Septia Nieng, "ANALISIS MANAJEMEN RESIKO APLIKASI MYPERTAMINA DENGAN MENGGUNAKAN ISO 31000," *INFOTECH journal*, vol. 9, no. 2, pp. 361–370, Jul. 2023, doi: 10.31949/infotech.v9i2.6232.

[13] P. Kanantyo, F. S. Papilaya, K. S. Wacana, J. Blotongan, K. Salatiga, and J. Tengah, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)," 2021. [Online]. Available: http://jurnal.mdp.ac.id

[14] F. Moi and I. G. A. N. Purnawirati, "Analisis Manajemen Risiko Pada Proyek Pembangunan Ruas Jalan Baru Waebetu – Tarawaja," *Jurnal Talenta Sipil*, vol. 4, no. 1, p. 79, Feb. 2021, doi: 10.33087/talentasipil.v4i1.52.

[15] V. Patrick, P. Wijaya, and A. D. Manuputty, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 2, pp. 1295–1307, 2022.

[16] S. Sarjana *et al.*, *Manajemen Risiko*. Kota Bandung: CV. MEDIA SAINS INDONESIA, 2022.