Jurnal Pendidikan Teknologi Informasi (JUKANTI)
Volume (7) No (2) Nopember 2024–eISSN : 2621-1467

ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN *FRAMEWORK* ISO 31000 PADA UNIT PEGADAIAN CABANG (UPC) RATAHAN

Cindy Claudya Turambi[1], Christ Rudianto[2]

[1,2] Fakultas Teknologi Informasi. Universitas Kristen Satya Wacana, Salatiga, Jawa Tengah

[1] 682020602@student.uksw.edu, [2] chris.rudianto@uksw.edu

ABSTRAK

Penelitian ini bertujuan untuk menganalisa risiko yang akan terjadi dan membangun strategi mitigasi yang efektif pada UPC Pegadaian Ratahan. Proses pengumpulan data menggunakan metode kualitatif. Dalam penelitian ini dilakukan analisis manajemen risiko dengan pedoman *framework* ISO 31000 yang terdiri dari identifikasi risiko, analisis risiko, evaluasi risiko, serta perlakuan risiko. Hasil yang ditemukan terdapat 14 risiko yang dapat mengganggu proses bisnis, namun dari ke-14 risiko tidak ada risiko dengan tingkatan *high risk*, terdapat 10 risiko tingkatan *medium risk*, dan 4 risiko tingkatan *low risk*. Untuk mengurangi dampak dari risiko yang telah diidentifikasi pada penelitian ini diterapkan strategi penanganan risiko, diantaranya Mitigasi risiko (Kebakaran, Penyalahgunaan hak akses, *Human Error*, *UI design* yang sulit dipahami, Listrik padam, Gangguan koneksi jaringan, *Hacking*, Pencurian data/perangkat keras), Eskalasi risiko (*Trouble web server*, *Server down*), Menghindari risiko (Kerusakan *hardware*, Data corrupt), Menerima risiko (Gempa bumi, Banjir). Penelitian ini diharapkan dapat membantu UPC Pedagaian Ratahan untuk meminimalisir risiko yang mungkin terjadi di masa mendatang.

Kata kunci *: framework ISO 31000, manajemen risiko, pegadaian, strategi penanganan risiko*

ABSTRACT

This research aims to analyze the risks that will occur and develop an effective mitigation strategy at UPC Pegadaian Ratahan. The data collection process uses qualitative methods. In this research, risk management analysis was carried out using the ISO 31000 framework guidelines which consist of risk identification, risk analysis, risk evaluation, and risk treatment. The results found there are 14 risks that can disrupt business processes, but of the 14 risks there are no risks with a high risk level, there are 10 medium risk level risks, and 4 low risk level risks. To reduce the impact of the risks that have been identified in this research, risk treatment strategies are applied, including Mitigating risks (Fire, Abuse of access rights, Human error, UI design that is difficult to understand, Power outages, Network connection problems, Hacking, Data theft/hardware), Risk escalation (Trouble web server, Server down), Avoiding risks (Hardware damage, Data corrupt), Accepting risks (Earthquake, Flood). This research is expected to help UPC Pegadaian Ratahan to minimize the risks that may occur in the future.

Kata kunci *: international organization for standardization 31000 framework, risk management, pegadaian, risk handling strategy*

1. PENDAHULUAN

Perkembangan teknologi yang sangat cepat dan pesat bukanlah suatu hal yang dapat dihindari, seluruh aspek kehidupan manusia saat ini bergantung pada teknologi. Teknologi informasi bisa dimanfaatkan dalam bentuk sistem informasi berbasis website yang dapat mengelola suatu informasi yang tepat dan berguna bagi perusahaan maupun organisasi [1].

Perusahaan maupun instansi yang menggunakan sistem informasi perlu mengelola keamanan informasi untuk melindungi aset teknologi informasi dari berbagai risiko. Salah satu contohnya adalah Unit Pelayanan Cabang (UPC) Pegadaian Ratahan. (UPC) Pegadaian Ratahan adalah salah satu kantor cabang PT. Pegadaian (Persero) dan merupakan anak usaha dari Bank Rakyat Indonesia yang bergerak di bidang gadai, pembiayaan fidusia, investasi emas, dan jasa lainnya baik secara konvensional maupun syariah [2]. Beberapa kegiatan kantor memanfaatkan teknologi informasi dalam menjalankan proses bisnis perusahaan. UPC Pegadaian Ratahan memiliki aset-aset teknologi seperti data, perangkat keras, jaringan, dan aplikasi-aplikasi yang menunjang hampir keseluruhan pekerjaan kantor.

Unit Pelayanan Cabang (UPC) Pegadaian Ratahan menghadapi masalah jaringan yang sering down akibat cuaca buruk dan kabel LAN digigit tikus, menghambat aktivitas dan memaksa penggunaan sistem manual. Selain itu, ketiadaan pegawai TI menyebabkan penundaan perbaikan infrastruktur karena harus dikonfirmasi ke kantor wilayah. Manajemen risiko diperlukan untuk meminimalisir dan mengurutkan risiko dari tingkat tertinggi hingga terendah.

Manajemen risiko merupakan penanggulangan risiko terutama risiko yang dihadapi oleh perusahaan atau instansi. Termasuk di dalamnya mengidentifikasi risiko-risiko dan menentukan besarnya risiko yang dihadapi, kemudian menyusun strategi guna memperkecil risiko tersebut [3]. Dari identifikasi permasalahan diatas, tujuan dari penelitian ini adalah untuk menganalisis risiko dan meminimalkan efek dari risiko tersebut pada Unit Pegadaian Cabang (UPC) Ratahan di masa depan. Penelitian ini berkonsentrasi pada pembuatan strategi mitigasi risiko yang efektif yang terdiri dari beberapa langkah praktis. Pertama, risiko diidentifikasi dan diklasifikasikan secara menyeluruh. Kedua, melakukan penilaian risiko yang sistematis menggunakan kerangka kerja ISO 31000. Ketiga, membuat strategi mitigasi yang

spesifik dan terukur untuk setiap kategori risiko; dan keempat, menerapkan strategi mitigasi secara bertahap sambil melakukan pengawasan dan evaluasi berkas. Dengan mengikuti langkah-langkah ini, penelitian diharapkan dapat menawarkan solusi praktis untuk membantu UPC Pegadaian Ratahan mengelola dan mengurangi risiko di masa mendatang.

Penelitian ini dilakukan dengan pendekatan menggunakan *framework* ISO 31000, yaitu sebuah panduan resmi yang telah distandarisasi oleh International Organization for Standardization (ISO) sebagai standar internasional. Tujuan dari ISO 31000 sendiri untuk menjadi pedoman bagi organisasi dalam menerapkan manajemen risiko pada berbagai keadaan bisnis guna menghadapi segala risiko yang akan muncul. Dalam pengelolaan risiko, ISO 31000 mengkategorikan risiko sesuai tingkat kepentingannya [4].

Analisis manajemen risiko menggunakan ISO 31000 oleh Sukma Arta Atmojo dkk (2020) di PT. Sumber Alfaria Trijaya menemukan 19 risiko, dengan 3 risiko ekstrem (kurangnya SDM, server down, kerusakan hardware), 7 risiko tinggi (dokumentasi kurang lengkap, keterlambatan program, kesalahan fungsi, kelalaian data, server mati, data corrupt, dan maintenance hardware), 7 risiko moderat (penyalahgunaan hak akses, pencurian perangkat, kurang komunikasi, akses informasi tidak bertanggung jawab, gempa bumi, kebakaran, dan gagal backup), serta 2 risiko rendah (tampilan aplikasi kurang user friendly dan banjir). [5].

Kajian berikutnya mengenai manajemen risiko menggunakan ISO 31000 dilakukan oleh Ferro Gartfain Punusingon dkk (2022) pada aplikasi SIMFONI PPA Di Dinas Pemberdayaan Perempuan dan Anak di Kabupaten Minahasa Tenggara. Penelitian ini bertujuan untuk menghindari risiko yang akan terjadi pada aplikasi yang membantu pendataan, pencatatan, dan monitoring kantor. Hasil dari penelitian ini terdapat 14 kemungkinan resiko diantaranya 4 resiko tinggi (*high)* yaitu: *human error*, *server down*, listrik padam, *data corrupt*. 4 resiko sedang (*medium)* yaitu: petir, pencurian data/perangkat keras, *trouble web server*, gangguan koneksi jaringan. Serta 6 resiko rendah (*low)* yaitu: gempa bumi, kebakaran, banjir, penyalahgunaan hak akses, *hacking*, kerusakan *hardware* [6].

Selain itu, Penelitian Miftakhatum (2022) tentang manajemen risiko ISO 31000 dilakukan pada Website Ecofo di Kesatuan Pemangkuan Hutan (KPH) Banyumas Timur, sebuah BUMN yang mengelola data tiket. Penelitian ini

bertujuan untuk mengidentifikasi kemungkinan risiko di masa depan serta cara penanganannya. Ditemukan 24 kemungkinan risiko, dengan 3 risiko tinggi (kegagalan sistem jaringan, overload database, server down), 10 risiko sedang (gempa bumi, kebakaran, listrik padam, penyalahgunaan hak akses, pegawai IT tidak mengikuti SOP, kegagalan software/hardware, masalah penyimpanan data, data corrupt, overheat perangkat), dan 11 risiko rendah (banjir, petir, debu, human error, pencurian perangkat, cybercrime, kesalahan teknis, pengunduran diri, pegawai sakit/cedera/meninggal, serangan virus). [7].

Penelitian dengan judul Risk Management Based IT Analysis Using ISO 31000 (Studi Kasus: PT Bawen Mediatama) yang ditulis oleh Evinia Evinia dan Melkior N. N. Sitokdana (2023) menganalisis risiko implementasi teknologi informasi di PT Bawen Mediatama dengan menggunakan kerangka kerja ISO 31000. Studi ini mengidentifikasi dua puluh kemungkinan bahaya dengan tingkat keparahan mulai dari ringan hingga sangat parah. Temuan utama dari penelitian ini adalah bahwa meskipun PT Bawen Mediatama telah menerapkan manajemen risiko, implementasinya belum optimal. Hal ini menunjukkan perlunya peningkatan dalam penerapan kerangka kerja manajemen risiko untuk memastikan bahwa semua potensi risiko dapat dikelola dengan lebih efektif dan efisien [8]

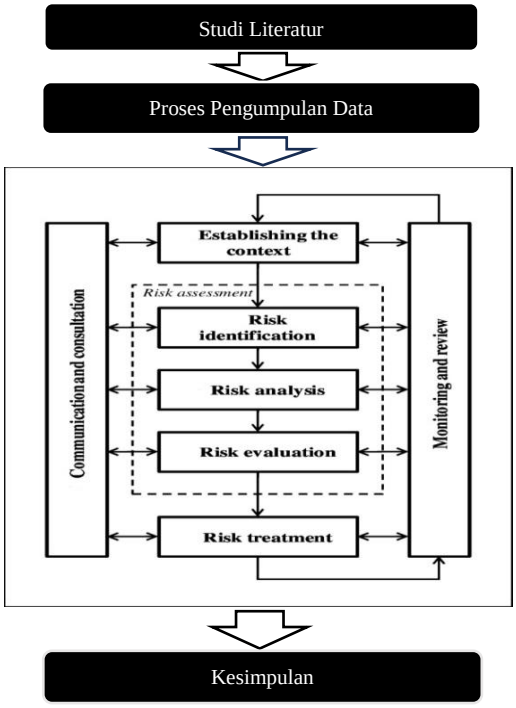
Penelitian oleh Pribadi, H. I., & Ernastuti, E dengan judul Manajemen Risiko Teknologi Informasi pada E-Recruitment di PT Pertamina (2020) menggunakan ISO 31000:2018 dan FMEA untuk menganalisis manajemen risiko teknologi informasi dalam proses penerimaan e-recruitment dengan menggunakan kerangka kerja ISO 31000:2018 dan FMEA. Studi ini menekankan betapa pentingnya menerapkan manajemen risiko yang efektif untuk memastikan kelancaran dan keamanan operasional sistem rekrutmen berbasis IT. Dengan mengidentifikasi dan mengevaluasi berbagai risiko teknis, operasional, dan keamanan, serta mengusulkan strategi mitigasi yang tepat, penelitian ini memberikan panduan yang berharga bagi praktik manajemen risiko di PT Pertamina dan menegaskan bahwa pendekatan sistematis seperti ISO 31000:2018 dapat mengurangi risiko. [9]

Berdasarkan penelitian-penelitian terdahulu sama-sama menggunakan *Framework* ISO 31000. Perbedaan dari penelitian ini dengan penelitian sebelumnya terletak pada objek penelitian adalah PT. Pegadaian Unit Cabang Pelayanan (UPC)

Ratahan, maka dari itu dalam penelitian ini diberikan judul "Analisis Manajemen Risiko Teknologi Informasi Menggunakan *Framework* ISO 31000 Pada Unit Cabang Pelayanan Cabang (UPC) Ratahan".

2. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif karena tujuan penelitian adalah untuk melakukan analisis risiko dan membangun strategi mitigasi yang efektif untuk Unit Pegadaian Cabang (UPC) Ratahan. Metode kualitatif memungkinkan untuk pengembangan teori baru dan rekomendasi praktis yang relevan dan dapat diterapkan untuk membantu UPC Pegadaian Ratahan meminimalisir bahkan menghilangkan risiko di masa mendatang. Metode ini juga memungkinkan pendekatan holistik untuk memahami risiko secara menyeluruh dan menyeluruh dalam konteks tertentu, memberikan fleksibilitas dalam pengumpulan data mendalam melalui wawancara dan menekankan pentingnya konteks dalam penilaian risiko. Oleh karena itu, metode kualitatif dipilih karena dapat memberikan wawasan kontekstual yang lebih kaya, fleksibel, dan akurat yang dibutuhkan untuk mencapai tujuan penelitian. Penelitian ini menggunakan dua tahap, pertama peneliti akan melakukan pencarian data dan informasi melalui wawancara langsung dengan narasumber dari kantor UPC Pegadaian Ratahan Kabupaten Minahasa Tenggara. Kedua peneliti mengolah data yang telah di dapat dari wawancara kemudian akan dianalisa berdasarkan kerangka kerja ISO 31000.



Gambar 1. Tahapan Penelitian

Dari tahapan penelitian pada gambar 1, dijelaskan sebagai berikut:

1. Studi Literatur

Tahap ini melibatkan pencarian referensi dari penelitian terdahulu yang serupa, output yang didapatkan untuk menambah wawasan tentang manajemen risiko di masa mendatang.

2. Proses Pengumpulan Data

Metode pengumpulan data yang digunakan adalah wawancara dengan pengelola Unit Pelayanan Cabang (UPC)

Pegadaian Ratahan. Output yang diharapkan adalah peneliti dapat mengidentifikasi aset teknologi informasi yang menghadapi ancaman dari dalam maupun luar serta menemukan risiko yang timbul di Unit Pelayanan Cabang (UPC)

Adapun tahapan penelitian *Framework* ISO 31000 yang digunakan peneliti, yaitu:

A. *Communication and consultation,* melakukan komunikasi konsultasi dengan dosen serta pihak perusahaan selama proses manajemen risiko untuk memastikan Unit Pelayanan Cabang (UPC) Pegadaian Ratahan memiliki pandangan yang sama dengan peneliti dan dapat membantu pengumpulan data.

B. *Establishing the context,* menentukan konteks analisis manajemen risiko TI di UPC Pegadaian Ratahan agar penilaian dan perlakuan risiko terfokus pada ruang lingkup tertentu, dengan menetapkan kriteria likelihood untuk frekuensi risiko dan dampak risiko.

C. *Risk Assessment,* dimana pada proses ini terdapat 3 tahapan, yaitu:

1. *Risk identification* adalah proses mengidentifikasi risiko dalam bisnis perusahaan. Sebelum itu, peneliti mengidentifikasi aset teknologi informasi di Unit Pelayanan Cabang (UPC) Pegadaian Ratahan. Tujuannya adalah untuk mengetahui semua risiko dari berbagai faktor, seperti manusia, alam, dan infrastruktur, agar dapat melindungi aset dari risiko yang akan terjadi.
2. *Risk analyst* Menentukan tingkat risiko dan menganalisis hasil identifikasi risiko dengan menilai risiko dan dampak risiko harian, mingguan, bulanan, hingga tahunan, membantu peneliti mengidentifikasi ancaman terhadap aset UPC Pegadaian Ratahan berdasarkan tiga faktor yang ditetapkan.
3. *Risk evaluation* merupakan proses menentukan risiko mana yang membutuhkan perlakuan dan prioritas, tujuan dari evaluasi risiko adalah untuk menentukan manajemen risiko serta membandingkan tingkat risiko dengan kriteria risiko, sehingga nantinya dapat diketahui risiko apa saja yang memiliki level tertinggi yang perlu ditangani secepatnya oleh UPC Pegadaian Ratahan [9].

D. *Risk Treatment,* bertujuan untuk memberikan rekomendasi tindakan atas kemungkinan risiko yang dapat digunakan sebagai acuan UPC Pegadaian Ratahan. Dengan harapan dapat membantu perusahaan untuk meminimalisir risiko yang akan terjadi.

E. *Monitoring and Review* tahap ini

memastikan implementasi manajemen risiko sesuai rencana dan menggunakan hasil monitoring serta review sebagai pertimbangan dalam proses manajemen risiko.

3. Proses Pengumpulan Data

Pada tahap akhir penelitian, peneliti menyimpulkan hasil analisis manajemen risiko di UPC Pegadaian Ratahan, dengan harapan hasil tersebut dapat menjadi acuan dalam mengelola risiko.

3. HASIL DAN PEMBAHASAN

Pada tahap ini peneliti melakukan penilaian risiko pada UPC Pegadaian Ratahan yang dilakukan sesuai pedoman analisis manajemen risiko ISO 31000. Proses penilaian risiko ini mencakup 3 proses: Identifikasi Risiko (*risk identification*), Analisis Risiko (*risk analysis*), Evaluasi Risiko (*risk evaluation*).

3.1 Penilaian Risiko (*Risk Assessment*)

3.1.1 Identifikasi Risiko (*risk identification*)

3.1.1.1 Identifikasi Aset

Tahap pertama penilaian risiko adalah identifikasi aset di UPC Pegadaian Ratahan, termasuk data, hardware, dan software, yang dilakukan melalui wawancara dengan pegawai pengelola. Aset teknologi informasi terkait dapat dilihat pada "Tabel 1".

Tabel 1. Identifikasi Aset UPC Pegadaian Ratahan

Komponen Sistem Informasi	Aset UPC Pegadaian Ratahan
Data	- Data surat bukti gadai - Data pembayaran - Data nasabah
Hardware	- 2 UPC (*Central Processing Unit*) - 3 Monitor - 1 Laptop - 3 Printer (1 printer untuk nota gadai yang digunakan oleh penaksir, 1 printer untuk nota pembayaran yang digunakan oleh kasir, 1 printer untuk fotocopy dan print data nasabah) - 1 Wifi LAN (Modem *MOBILE CONNECTIVITY SERVICES*, Router CISCO) - 1 STAVOLT - 4 CCTV - 1 Timbangan Digital - GENSET
Software	- Web base PASSION (untuk pencairan dan pembayaran gadai) - Web base PRIME (untuk non gadai)

3.1.1.2 Identifikasi Risiko

Setelah mengidentifikasi aset di UPC Pegadaian Ratahan, ditemukan 14 risiko yang dikelompokkan berdasarkan tiga faktor: Alam/Lingkungan, Manusia, dan Sistem/Infrastruktur. Setiap risiko diberi nomor ID, seperti pada Tabel 2.

Tabel 2. Identifikasi Risiko

ID	Risiko	Faktor
C01	Gempa Bumi	Alam/Lingkungan
C02	Kebakaran	
C03	Banjir	
C04	Penyalahgunaan Hak Akses	Manusia
C05	Human Error	
C06	Hacking	
C07	Pencurian Data/Perangkat Keras	
C08	UI Design Yang Sulit di Pahami	Sistem dan Infrastruktur
C09	Trouble Web Server	
C10	Server Down	
C11	Listrik Padam	
C12	Gangguan Koneksi Jaringan	
C13	Kerusakan Hardware	
C14	Data Corrupt	

3.1.1.3 Identifikasi Dampak Risiko

Setelah melakukan identifikasi risiko, tahap ketiga adalah melakukan identifikasi dampak risiko dan implikasi jangka panjang yang akan muncul pada UPC Pegadaian Ratahan dari risiko yang sudah diidentifikasi. Berikut identifikasi dampak risiko dapat dilihat pada “Tabel 3”.

Tabel 3. Identifikasi Dampak Risiko

ID	Risiko	Implikasi Jangka Pendek	Implikasi Jangka Panjang
C01	Gempa Bumi	Kerusakan perangkat, gangguan operasional sementara, kehilangan data, dan kebutuhan mendesak untuk perbaikan	Pemulihan sistem, peninjauan ketahanan infrastruktur TI, penyesuaian prosedur manajemen risiko, dan pengeluaran tambahan untuk perbaikan dan penguatan sistem.
C02	Kebakaran	Kerusakan perangkat TI, gangguan operasional, kehilangan data, dan	Pemulihan sistem yang memerlukan waktu dan biaya, peninjauan ketahanan infrastruktur TI, penyesuaian prosedur manajemen risiko, dan

		kebutuhan mendesak untuk tindakan darurat	pengeluaran tambahan untuk perbaikan dan penguatan sistem.
C03	Banjir	Kerusakan perangkat TI, gangguan akses data, dan kehilangan data	Pemulihan sistem yang memakan waktu dan biaya, peninjauan ketahanan infrastruktur TI terhadap banjir, penyesuaian prosedur manajemen risiko, serta pengeluaran tambahan untuk perbaikan dan penguatan sistem.
C04	Penyalahgunaan Hak Akses	Potensi kebocoran data, gangguan operasional, dan kerusakan reputasi akibat akses tidak sah	Kerusakan yang lebih luas pada integritas data, memerlukan evaluasi dan perbaikan sistem keamanan TI, serta penyesuaian prosedur manajemen risiko untuk mencegah kejadian serupa di masa depan
C05	Human Error	Kesalahan operasional yang dapat menyebabkan gangguan sistem dan kehilangan data	Kebutuhan untuk memperbaiki kesalahan, memperbarui prosedur dan pelatihan, meningkatkan sistem kontrol untuk mencegah kesalahan serupa di masa depan,yang memerlukan waktu dan biaya tambahan.
C06	Hacking	Potensi kebocoran data sensitif, gangguan operasional, dan kerusakan reputasi	Kebutuhan untuk memperbaiki dan memperkuat sistem keamanan TI, melakukan audit keamanan menyeluruh, penyesuaian kebijakan dan prosedur manajemen risiko yang memerlukan investasi signifikan.
C07	Pencurian Data/Perangkat Keras	Kerugian finansial, kehilangan data penting, gangguan operasional, dan potensi kerusakan reputasi	Pemulihan data, mengganti perangkat yang hilang, memperkuat keamanan, dan menyesuaikan prosedur manajemen risiko, dan memerlukan waktu dan biaya tambahan.
C08	UI Design Yang Sulit di Pahami	Kesulitan operasional, kesalahan penggunaan, dan penurunan produktivitas karyawan.	Kebutuhan untuk perbaikan UI, pelatihan staf, dan peningkatan efisiensi system yang memerlukan waktu dan biaya tambahan serta potensi gangguan terhadap proses bisnis.
C09	Trouble Web Server	Aplikasi PASSION tidak dapat di akses dan aktivitas kantor sedikit terhambat namun aktivitas utama tidak terganggu	Perbaikan dan peningkatan infrastruktur server, melakukan audit sistem, serta implementasi langkah-langkah pencegahan untuk menghindari masalah serupa di masa depan yang memerlukan investasi tambahan dalam waktu dan biaya.
C10	Server Down	Server data base bermasalah mengakibatkan aktivitas kantor terhambat	Perbaikan dan peningkatan infrastruktur server, audit sistem untuk mencegah masalah serupa, serta penyesuaian kebijakan manajemen risiko, yang melibatkan waktu dan biaya tambahan.
C11	Listrik Padam	Aktivitas kantor sedikit terhambat namun aktivitas utama tidak terganggu	Perlunya investasi dalam solusi cadangan daya seperti UPS atau generator, peninjauan kebijakan manajemen risiko, dan peningkatan infrastruktur untuk memastikan ketahanan terhadap pemadaman listrik di masa depan yang memerlukan biaya tambahan dan waktu.
C12	Gangguan Koneksi Jaringan	Aktivitas kantor sedikit terhambat namun aktivitas utama tidak terganggu	Perbaikan dan peningkatan infrastruktur jaringan, evaluasi penyebab gangguan, serta penyesuaian prosedur manajemen risiko untuk mencegah masalah serupa di masa depan yang melibatkan investasi tambahan dalam waktu dan biaya.
C13	Kerusakan Hardware	Menyebabkan gangguan pada proses kinerja sehingga aktivitas kantor terhambat	Penggantian atau perbaikan perangkat, peningkatan ketahanan hardware, dan penyesuaian prosedur pemeliharaan serta manajemen risiko memerlukan waktu dan biaya tambahan.

C14	Data Corrupt	Tidak dapat mengakses data sehingga aktivitas kantor terhenti	Pemulihan data, perbaikan sistem, peningkatan prosedur backup dan pemeliharaan data, serta penyesuaian kebijakan manajemen risiko untuk mencegah kejadian serupa, yang memerlukan waktu dan biaya tambahan.

3.1.2 Analisis Risiko (*Risk Analysis*)

Setelah melakukan identifikasi risiko, selanjutnya masuk pada proses analisis risiko. Pada tahap ini dilakukan analisis terhadap risiko yang telah diidentifikasi sebelumnya. Tahap ini memiliki 2 tabel kriteria yaitu *Impact* dan *Likelihood* yang menjadi acuan pada tahap analisis risiko. Tabel 4 berisi tabel kriteria *Impact* yang mencakup 5 kriteria berdasarkan seberapa banyak risiko yang dapat terjadi dalam jangka waktu tertent

Tabel 4. Kriteria *impact*

Nilai	Kriteria	Keterangan
1	*Insignificant*	Tidak mengganggu aktivitas kantor
2	*Minor*	Aktivitas kantor sedikit terhambat namun aktivitas inti tidak terganggu
3	*Moderate*	Menyebabkan gangguan pada kinerja sehingga jalannya aktivitas kantor terhambat
4	*Major*	Menghambat hampir seluruh aktivitas kantor
5	*Catastrophic*	Aktivitas kantor berhenti karena proses kinerja mengalami gangguan total

Selanjutnya pada Tabel 5 terdapat tabel nilai *likelihood* merupakan dampak jika risiko tersebut terjadi di kantor UPC Pegadaian Ratahan. Dalam tabel penilaian *likelihood* mempunyai 5 kriteria dampak yang mungkin terjadi, dibedakan berdasarkan yang tidak berpengaruh bagi kinerja kantor hingga dampak yang paling mempengaruhi kinerja kantor UPC Pegadaian Ratahan.

Tabel 5. Kriteria *Likelihood*

Nilai	Kriteria	Keterangan	Frekuensi Kejadian
1	*Rare*	Resiko tersebut hampir tidak pernah terjadi	>2 tahun
2	*Unlikely*	Resiko tersebut jarang terjadi	1-2 tahun
3	*Possible*	Resiko tersebut kadang terjadi	7-12 bulan

4	*Likely*	Resiko tersebut sering terjadi	4-6 bulan
5	*Certain*	Resiko tersebut pasti terjadi	1-3 bulan

Setelah menentukan nilai *Impact* pada Tabel 4 dan *Likelihood* pada Tabel 5, dilakukan penilaian terhadap 14 risiko yang teridentifikasi, dengan acuan dari tabel-tabel tersebut. Hasil penilaian risiko ditunjukkan pada Tabel 6.

Tabel 6. Penilaian Terhadap Risiko

ID	Risiko	Likelihood	Impact
C01	Gempa Bumi	2	2
C02	Kebakaran	1	4
C03	Banjir	1	3
C04	Penyalahgunaan Hak Akses	3	3
C05	Human Error	4	2
C06	Hacking	1	3
C07	Pencurian Data/Perangkat Keras	1	3
C08	UI Design Yang Sulit di Pahami	3	2
C09	Trouble Web Server	4	2
C10	Server Down	4	2
C11	Listrik Padam	5	2
C12	Gangguan Koneksi Jaringan	5	2
C13	Kerusakan Hardware	4	3
C14	Data Corrupt	1	4

3.1.3 Evaluasi Risiko (*Risk Evaluation*)

Proses terakhir dalam penilaian risiko (*risk assessment*) adalah evaluasi risiko. pada proses ini menggunakan acuan berupa matriks evaluasi risiko berdasarkan arahan kerangka kerja dari ISO 31000 yang dikategorikan menjadi 3 level risiko yaitu : *low, medium, high.* Tabel matriks evaluasi risiko dapat dilihat pada “Tabel 7” dibawah ini.

Tabel 7. Matriks 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
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*

Kemudian, risiko-risiko yang telah dianalisis dalam proses sebelumnya dibandingkan berdasarkan nilai Impact dan Likelihood-nya. Risiko-risiko tersebut dimasukkan ke dalam tabel matriks risiko sesuai dengan pemetaan tabel yang telah ditentukan. Hasil dari proses ini dapat dilihat pada "Tabel 8" di bawah, yang menunjukkan risiko yang telah dimasukkan ke dalam tabel matriks evaluasi.

Tabel 8. Matriks Evaluasi Risiko Berdasarkan *Impact* dan *Likelihood*

Likelihood	*Certain*	5		**C12 C11**			
	Likely	4		C05 C09 C10	C13		
	Possible	3		C08	C04		
	Unlikely	2		C01			
	Rare	1			C03 C06 C07	C02 C14	
Impact			1	2	3	4	5
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*

Sesudah semua risiko-risiko dikategorikan level resikonya sesuai dengan nilai impact dan likelihood, pada tabel 9 dibawah dibuat pengelompokan 14 risiko yang disesuaikan dengan tingkatan level high, medium, dan low berdasarkan data pada tabel 8 diatas.

Tabel 9. Klasifikasi Risiko Berdasarkan *risk level*

ID	Risiko	Likelihood	Impact	*Risk Level*
C02	Kebakaran	1	4	*Medium*
C04	Penyalahgunaan Hak Akses	3	3	*Medium*
C05	Human Error	4	2	*Medium*
C08	UI Design Yang Sulit di Pahami	3	2	*Medium*
C09	Trouble Web Server	4	2	*Medium*
C10	Server Down	4	2	*Medium*
C11	Listrik Padam	5	2	*Medium*
C12	Gangguan Koneksi Jaringan	5	2	*Medium*
C13	Kerusakan Hardware	4	3	*Medium*
C14	Data Corrupt	1	4	*Medium*

C01	Gempa Bumi	2	2	*Low*
C03	Banjir	1	3	*Low*
C06	Hacking	1	3	*Low*
C07	Pencurian Data/Perangkat Keras	1	3	*Low*

Dari "Tabel 9" diatas diperoleh 10 risiko dengan tingkat *medium* yaitu: C02, C04, C05, C08, C09, C10, C11, C12, C13, C14. Dan 4 risiko dengan tingkat *low* yaitu: C01, C03, C06 dan C07.

3.2 Perlakuan Risiko (*Risk Treatment*)

Proses akhir dalam penelitian ini setelah melalui 3 proses tahapan *risk assessment* adalah perlakuan risiko atau *risk treatment.* Untuk mengurangi atau menghilangkan dampak dari risiko terdapat beberapa strategi penanganan risiko diantaranya sebagai berikut:

- Eskalasi Risiko, merupakan risiko yang berada di luar wewenang maka dilakukan dengan melimpahkan tanggung jawab penanganan risiko ke unit yang lebih tinggi.
- Menerima Risiko yaitu menerima risiko dengan tidak melakukan perlakuan apapun hanya mengontrol risiko yang ada.
- Menghindari Risiko artinya tidak melakukan kegiatan yang mengakibatkan risiko
- Transfer Risiko merupakan tindakan memindahkan sebagian risiko ke individu atau organisasi lain. Namun tidak berarti tingkat risiko berkurang.
- Mitigasi yang bertujuan untuk mengurangi risiko yang timbul

Pada tahap ini, Peneliti mengusulkan tindakan untuk setiap risiko yang telah diidentifikasi di UPC Pegadaian Ratahan. Rincian usulan dan kategori penanganan risiko dapat dilihat pada Tabel 10. Usulan ini bertujuan untuk meminimalisir risiko sehingga operasional aplikasi dan aktivitas kantor dapat berjalan optimal..

Tabel 10. Perlakuan Terhadap Risiko

ID	*Risk Level*	Opsi Perlakuan Risiko	Perlakuan Risiko	Sumber Risiko
C02	*Medium*	Mitigasi Risiko	Meletakkan server di tempat yang lebih aman serta menyiapkan server Cadangan di Lokasi yang berbeda	Internal
C04	*Medium*	Mitigasi Risiko	Menerapkan manajemen keamanan informasi untuk membatasi user dalam mengakses aplikasi, melakukan *update password* secara berkala	Internal
C05	*Medium*	Mitigasi Risiko	Melakukan *training* untuk pegawai baru	Internal
C08	*Medium*	Mitigasi Risiko	Melakukan pelatihan tentang penggunaan aplikasi dengan fitur yang ada	Internal
C09	*Medium*	Eskalasi Risiko	Melakukan pengecekan pada *web server*, *domain* dan *hosting* atau melaporkan kepada pihak IT yang ada kantor wilayah	Internal
C10	*Medium*	Eskalasi Risiko	Melakukan monitoring secara berkala pada server atau melaporkan kepada bagian IT	Internal
C11	*Medium*	Mitigasi Risiko	Menggunakan genset yang ada, serta menyiapkan UPS (*Uninterruptible Power Supply*) sebagai penunjang sementara.	Eksternal
C12	*Medium*	Mitigasi Risiko	Menyediakan operator internet cadangan dengan memilih jenis ISP berbeda dari yang sudah ada.	Internal
C13	*Medium*	Menghindari Risiko	Melakukan perawatan secara berkala dan mengganti *Hardware* yang sudah rusak	Internal
C14	*Medium*	Menghindari Risiko	Melakukan *backup* data secara rutin dan rutin melakukan pembersihan data-data agar *server* tetap stabil	Internal
C01	*Low*	Menerima Risiko	Menyimpan aset atau data pada tempat aman	Eksternal
C03	*Low*	Menerima Risiko	Meletakkan alat infrastruktur pada tempat yang aman dari banjir	Eksternal
C06	*Low*	Mitigasi Risiko	Mengganti *password* secara rutin serta membatasi maksimal kesalahan *password* dan memastikan *system security* pada aplikasi-aplikasi yang ada berjalan benar.	Eksternal
C07	*Low*	Mitigasi Risiko	Meningkatkan keamanan dengan memperbanyak titik pemasangan CCTV pada bagian tertentu	Eksternal

4. KESIMPULAN

Berdasarkan penelitian yang dilakukan, tujuan analisis manajemen risiko menggunakan ISO 31000 pada UPC Pegadaian Ratahan telah tercapai. Dari hasil identifikasi, ditemukan 14 risiko yang dapat menghambat kinerja kantor. Tidak ada risiko dengan tingkatan high risk, 10 risiko dengan tingkatan medium risk, dan 4 risiko dengan tingkatan low risk. Strategi perlakuan risiko yang digunakan meliputi mitigasi risiko untuk 8 risiko, eskalasi risiko untuk 2 risiko, menerima risiko untuk 2 risiko, dan menghindari risiko untuk 2 risiko.

Kelebihan analisis manajemen risiko menggunakan framework ISO 31000 adalah adanya panduan lengkap dalam mengelola risiko, yang membantu pelaksanaan penelitian. Namun, penelitian menghadapi kendala seperti keterbatasan sumber daya dan staf UPC Pegadaian Ratahan dalam pemahaman TI, serta kurangnya keterampilan dalam mengelola analisis risiko. Pengelolaan manajemen risiko membutuhkan pengetahuan TI dan data empiris untuk mendukung proses identifikasi. Penelitian ini diharapkan dapat membantu UPC Pegadaian Ratahan dalam menangani risiko yang telah direkomendasikan, sehingga dapat meminimalisir risiko di masa mendatang.

DAFTAR PUSTAKA

[1] Sutabri, T. (2014). Pengantar teknologi informasi. Yogyakarta: Andi Offset.

[2] Pegadaian. Sejarah Pegadaian. Diakses dari https://www.pegadaian.co.id/profile/sejarah-pegadaian.

[3] Subagyo, A., Simanjutak, R., & Bukit, A. I. (2020). DASAR-DASAR MANAJEMEN RISIKO. www.mitrawacanamedia.com.

[4] Fachrezi, M. I., Dwika Cahyono, A., & Tanaem, P. F. (2021). Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga. Jurusan Sistem Informasi, 8(2). Diakses dari http://jurnal.mdp.ac.id.

[5] Atmojo, S. A., & Manuputty, A. D. (2020). Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office (Vol. 7, Issue 3). Diakses dari http://jurnal.mdp.ac.id.

[6] Punusingon, F. G., & Sitokdana, M. N. (2022). ANALISIS MANAJEMEN RESIKO APLIKASI SIMFONI PADA DINAS PPA DI KAB. MINAHASA TENGGARA MENGGUNAKAN ISO 31000 (Vol. 4, Issue 2).

[7] Miftakhatun, M. (2020). Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000. Journal of Computer Science and Engineering (JCSE), 1(2), 128–146. https://doi.org/10.36596/jcse.v1i2.76

[8] Evinia, E., & Sitokdana, M. N. N. (2023). Risk Management Based IT Analysis Using ISO 31000 (Case Study: PT Bawen Mediatama). Journal of Information Systems and Informatics, Universitas Kristen Satya Wacana. https://doi.org/10.51519/journalisi.v5i1.420.

[9] Natalie, D. P., & Manuputty, A. D. (2022). Analisis Manajemen Risiko Teknologi Informasi dengan ISO 31000:2018 pada PT Bayu Buana Tbk. JURIKOM (Jurnal Riset Komputer), 9(5), 1290. https://doi.org/10.30865/jurikom.v9i5.4797.

[10] Ramadhan, D. L., Febriansyah, R., & Dewi, R. S. (2020). Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ. JURIKOM (Jurnal Riset Komputer), 7(1), 91. https://doi.org/10.30865/jurikom.v7i1.1791.