Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2018 pada INLISlite (*Integrated Library System*) di Dinas Perpustakaan dan Kearsipan Kota Salatiga

FX Mario R. M. Junior, Johan Jimmy Carter Tambotoh
Program Studi Sistem Informasi
Universitas Kristen Satya Wacana, Jl. Diponegoro
Email : 682020118@student.uksw.edu

ABSTRAK

Dalam era digital yang semakin berkembang, penerapan teknologi informasi menjadi krusial bagi organisasi, termasuk di sektor perpustakaan dan kearsipan. Teknologi tidak hanya memfasilitasi efisiensi pelayanan publik, tetapi juga membawa tantangan berupa risiko-risiko yang perlu dikelola secara efektif untuk menjaga keberlanjutan operasional. Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan menilai risiko pada Dinas Perpustakaan dan Kearsipan Kota Salatiga dalam penggunaan aplikasi INLISlite (Integrated Library System) dengan pendekatan Framework ISO 31000:2018. Metode yang digunakan meliputi studi kasus dengan pendekatan kualitatif, mengidentifikasi risiko dari faktor alam, manusia, dan sistem, yang dapat mengancam keberlangsungan operasional perpustakaan. Hasil penelitian menunjukkan bahwa terdapat berbagai risiko signifikan seperti kegagalan server, serangan hacking, dan kesalahan manusia, yang memerlukan strategi mitigasi. Rekomendasi dalam penelitian ini mencakup pembaruan sistem, peningkatan kapasitas server, serta pelatihan bagi staf untuk meminimalkan risiko. Dengan penerapan ISO 31000:2018, perpustakaan dapat mengelola risiko secara lebih sistematis, sehingga meningkatkan keamanan dan efektivitas sistem informasi yang digunakan.

Kata Kunci : INLISlite, ISO 31000:2018, Manajemen Risiko, Mitigasi Risiko, Perpustakaan

ABSTRACT

In the growing digital era, the application of information technology is crucial for organizations, including in the library and archives sector. Technology not only facilitates the efficiency of public services, but also brings challenges in the form of risks that need to be managed effectively to maintain operational sustainability. This study aims to identify, analyze, and assess the risks in the library and Archives Office of Salatiga city in the use of INLISlite (Integrated Library System) application with ISO 31000:2018 Framework approach. The methods used include case studies with a qualitative approach, identifying risks from natural, human, and system factors, which can threaten the operational stability of the library. The results show that there are significant risks such as server failures, hacking attacks, and human error, which require mitigation strategies. Recommendations in this study include System Improvement, server capacity improvement, and training for staff to minimize risks. With the implementation of ISO 31000: 2018, libraries can manage risks more systematically, thereby increasing the security and effectiveness of the information systems used.

Keywords **:** INLISlite, ISO 31000: 2018, *Library, Risk Management, Risk Mitigation.*

1. PENDAHULUAN

Pada era digital saat ini, perkekmbangan teknologi informasi menjadi tulang punggung bagi organisasi dalam menjalankan operasinya. Terutama di sektor pelayanan publik seperti perpustakaan dan kearsipan, teknologi informasi dapat memberikan pelayanan yang efisien dan terintegrasi bagi masyarakat. Termasuk dalam pengelolaan INLISlite (Integrated Library System) yang membuat pengelolaan informasi di perpustakaan menjadi lebih efisien dan akurat. Namun, dengan kecanggihan teknologi juga dapat menimbulkan risiko-risiko yang harus dikelola secara efektif untuk memastikan keberlangsungan dan keamanan sistem informasi (Aisyah et al., 2024).

Mengelola risiko sistem informasi/teknologi informasi di suatu perusahaan atau instansi akan memberikan nilai tambah pada aset teknologi informasi tersebut, menjadikannya sebagai alat yang efektif dan efisien bagi keberlangsungan operasional dan pertumbuhan organisasi (Andika & Wijaya, 2022). Menurut Harefa & Hartomo (2022), perusahaan yang mampu mengelola risiko SI/TI dengan baik akan mengalami proses bisnis yang lebih efektif dan efisien, memungkinkan mereka mencapai tujuan bisnis dengan lebih baik. Kesuksesan sebuah perusahaan tidak hanya tergantung pada inovasi teknologi yang diterapkan, tetapi juga pada kemampuan mereka guna melakukan identifikasi, evaluasi, dan mengelola risiko yang berkaitan dengan teknologi informasi.

Risiko bisa datang kapan saja dan dimana saja maka dari itu diperlukan manajemen risiko, manajemen risiko adalah proses manajemen mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko dalam suatu perusahaan atau instansi (Sarjana, 2020). Setiap perusahaan tidak luput dari risiko, dan setiap risiko harus dikelola dengan benar. Manajemen risiko harus menjadi proses pengembangan yang berkelanjutan dan harus menjadi bagian dari budaya organisasi atau perusahaan. Tujuan utama dari manajemen risiko yaitu mengurangi atau meminimalkan dampak negatif dari risko dengan memaksimalkan peluang yang ada. Meskipun risiko tidak dapat dieliminasi, namun risiko SI/TI dapat diminimalisir, sehingga manfaat manajemen risiko tidak mengganggu aktivitas proses bisnis (Anita et al., 2023).

Di bidang perpustakaan, teknologi informasi (TIK) memiliki pengaruh yang signifikan karena memungkinkan akses mudah dan praktis ke informasi seperti teks, audio, video, dan multimedia. Selain itu, pengelolaan bahan pustaka menjadi lebih

mudah bagi pustakawan dan menjadikan profesi mereka lebih profesional. Namun, tidak dapat dipungkiri peranan TIK juga dapat memberikan dampak risiko-risiko seperti *data corrupt, system error*, kehilangan data, mutilasi data, pencurian data dan lai-lain yang mengganggu proses kerja perpustakaan dan kenyamanan pengguna (Supriatin & Wijaya, 2022).

Dinas Perpustakaan dan Kearsipan Kota Salatiga menggunakan Sistem Informasi untuk membantu dalam meningkatkan efektivitas kerja dan efisiensi waktu serta hemat biaya dalam kegiatan perpustakaan. contoh nya yaitu INLISlite yang diciptakan sejak tahun 2011 oleh Perpustakaan Nasional Republik Indonesia. . Pada tahun 2015 dilakukan pengembangan pada aplikasi INLISlite versi 3.0 yang sebelumnya versi 2.1.2. Dengan adanya INLISlite dapat mempermudah masyarakat unutk memproleh informasi mengenai katalog buku tanpa perlu datang ke perpustakaan. selain itu, anggota perpustakaan dapat melakukan booking buku kapanpun dan dimana pun dengan internet namun, tidak semua pustakawan bisa memanfaatkan teknologi ini sehingga perlu diadakan pelatihan mengenai penggunaan INLISlite untuk mencegah risiko seperti human error (Fatmawati, 2020).

Risiko, menurut Kristiana (2022) adalah peristiwa tidak pasti yang dapat menimbulkan dampak positif maupun negatif pada tujuan organisasi. Risiko ini menciptakan peluang bagi terjadinya peristiwa dengan konsekuensi yang dapat mengakibatkan kerugian. Risiko didefinisikan sebagai ketidakpastian atau ancaman yang berpotensi memengaruhi pencapaian tujuan organisasi dan digunakan untuk menggambarkan kemungkinan hasil dari suatu peristiwa, di mana masa depan tidak dapat dipastikan dan berbagai hasil yang mungkin terjadi tidak selalu diketahui. Hanafi (mengelompokkan risiko menjadi dua jenis, yaitu risiko murni dan risiko spekulatif. Risiko murni (pure risk) mengacu pada situasi di mana hanya ada kemungkinan kerugian, seperti kecelakaan, kebakaran, dan bencana alam (Hanafi, 2021). Karakteristik dari risiko murni adalah dapat diasuransikan, sehingga organisasi bisa mengambil langkah pencegahan seperti membeli asuransi untuk mengurangi dampak finansial. Di sisi lain, risiko spekulatif melibatkan situasi yang memungkinkan adanya keuntungan maupun kerugian, seperti dalam investasi saham dan kegiatan bisnis. Dalam hal ini, risiko spekulatif tidak hanya menimbulkan potensi kerugian, tetapi juga peluang keuntungan bagi pihak tertentu; misalnya, penurunan penjualan suatu perusahaan yang

merugikan perusahaan tersebut, namun dapat menguntungkan kompetitor (Tabun et al., 2023).

Menurut Sri Sarjana, manajemen risiko adalah proses dalam organisasi yang bertujuan untuk mengidentifikasi, menilai, dan mengendalikan berbagai ancaman serta tantangan yang dapat menghambat pencapaian tujuan organisasi (Sarjana et al., 2022). Ancaman ini bisa berasal dari ketidakpastian finansial, kewajiban hukum, kesalahan dalam strategi bisnis, kecelakaan, atau bencana alam. Di era modern, privasi dan ancaman terhadap keamanan teknologi informasi menjadi perhatian utama bagi organisasi, sehingga penting bagi mereka untuk mengadopsi rencana manajemen risiko yang memungkinkan identifikasi dan penanganan ancaman agar dapat mengambil tindakan preventif. Manajemen risiko juga melibatkan prediksi dan evaluasi risiko finansial yang diiringi dengan penentuan langkah-langkah untuk menghindari atau meminimalkan dampaknya. Ancaman tersebut dapat timbul dari berbagai sumber, seperti ketidakpastian finansial, kewajiban hukum, atau bahkan bencana alam. Ancaman keamanan siber menjadi prioritas dalam manajemen risiko teknologi informasi karena dapat memengaruhi kelangsungan organisasi (Royyan, 2023). Oleh sebab itu, rencana manajemen risiko melibatkan proses pengendalian ancaman terhadap semua aspek bisnis, termasuk perlindungan data perusahaan, informasi pelanggan, dan kekayaan intelektual. Baik bisnis besar maupun kecil menghadapi potensi risiko kejadian tak terduga yang dapat memengaruhi stabilitas finansial. Manajemen risiko membantu organisasi dalam mengidentifikasi, merencanakan, mempersiapkan, dan melindungi diri terhadap berbagai skenario buruk dalam jangka panjang, serta memberikan informasi penting terkait ancaman yang ada. Tanpa manajemen risiko, bisnis akan lebih rentan terhadap masalah karena tidak mampu mengantisipasi tingkat risiko yang dihadapi. Rencana manajemen risiko yang tepat juga berkontribusi pada keberlanjutan perusahaan dalam jangka panjang (Sigalingging et al., 2024).

Oleh karena itu, manajemen risiko berperan penting sebagai elemen strategis dalam upaya keberlanjutan organisasi dan berfokus pada pencegahan serta mitigasi bahaya. Rencana manajemen risiko yang baik tidak hanya membantu dalam menghindari kerugian tetapi juga mendukung pengambilan keputusan yang lebih baik di tingkat manajerial (Agil et al., 2023).

Teknologi Informasi (TI) saat ini memiliki peran penting dalam mendukung operasional berbagai perusahaan dan menjadi komponen utama dalam pengelolaan proses bisnis. Namun, TI juga menghadapi berbagai risiko yang dapat mengancam sistem serta data informasi, sehingga diperlukan proses identifikasi dan pengelolaan risiko yang efektif untuk mengurangi dampaknya serta melindungi keuntungan perusahaan. Proses manajemen risiko ini bersifat berulang dan berkesinambungan, mengingat lingkungan bisnis yang terus berubah dan menimbulkan ancaman baru. Opsi pengendalian yang diterapkan dalam manajemen risiko harus mempertahankan keseimbangan antara produktivitas, biaya, efektivitas pengendalian, serta nilai dari sumber daya informasi yang dilindungi. Manajemen risiko TI bertujuan untuk memberikan panduan kepada eksekutif dan manajer dalam mengajukan pertanyaan kritis, membuat keputusan yang lebih bijak dan sesuai dengan risiko yang dihadapi, serta membantu organisasi dalam mengelola risiko secara efisien (Amiruddin et al., 2023). Selain itu, manajemen risiko TI dapat menghemat waktu, biaya, dan sumber daya dengan menyediakan alat yang relevan untuk mengelola risiko bisnis, mengintegrasikan manajemen risiko TI ke dalam kerangka manajemen risiko perusahaan secara keseluruhan, serta membantu para pemimpin memahami risiko dan tingkat toleransi organisasi terhadap risiko. Manajemen risiko TI juga menawarkan panduan praktis yang disesuaikan dengan kebutuhan kepemimpinan perusahaan di seluruh dunia.

Framework ISO 31000:2018 tentang manajemen risiko adalah suatu panduan yang menyediakan struktur untuk mengelola risiko dalam suatu organisasi. ISO 31000 adalah pedoman penerapan risiko yang terdiri dari tiga komponen, yaitu prinsip, kerangka kerja, dan proses. *International Organization Form Standardization* (ISO) adalah lembaga yang bertanggung jawab untuk membuat pedoman ini. Pada tahun 2018, ISO mengeluarkan struktur manajemen risiko terbarunya, ISO 31000:2018, yang disebut sebagai "*risk management guide*". Struktur ini merupakan penyederhanaan dari ISO 31000:2009, sehingga poin-poinnya lebih ringkas dan mudah dipahami. Perbedaan antara versi 2009 dan versi 2018 terletak pada bagaimana elemen prinsip, kerangka kerja, dan proses dibahas. Pada versi 2009, ketiga elemen tersebut digambarkan sebagai rangkaian unsur yang berurutan, tetapi pada versi 2018, ketiga elemen tersebut digambarkan sebagai elemen yang terbuka dan saling berhubungan (Pratama & Pratika, 2020). Proses manajemen risiko yang dijelaskan dalam framework ini melibatkan

langkah-langkah seperti mengidentifikasi aset dan potensi risiko yang terkait, melakukan analisis risiko yang komprehensif, dan mengevaluasi risiko untuk menentukan dampaknya pada operasional organisasi. Aktivitas manajemen risiko ini mewakili upaya dari manajemen untuk memantau dan mengontrol risiko yang mungkin timbul dalam aktivitas operasional perusahaan, dengan melakukan analisis mendalam, evaluasi terhadap kemungkinan dampak, serta merencanakan strategi mitigasi untuk mengatasi risiko yang diidentifikasi. ISO 31000:2018 menjadi hal yang sangat penting dalam mengelola risiko di sebuah instansi Oleh karena itu, penting bagi Dinpersip Salatiga untuk memiliki sistem manajemen risiko TI yang kuat dan terstruktur untuk melindungi aset-aset informasi mereka, memastikan keberlangsungan operasional, dan meminimalkan dampak dari potensi ancaman.

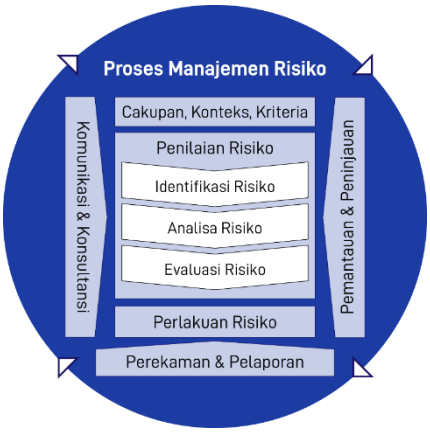
Rumusan masalah dalam penelitian ini didasarkan pada latar belakang yang telah dijelaskan sebelumnya, yaitu: bagaimana cara mengidentifikasi dampak serta menilai risiko yang ada pada Dinas Perpustakaan dan Kearsipan Kota Salatiga, serta apa rekomendasi dan langkah mitigasi risiko yang dapat diterapkan berdasarkan Framework ISO 31000:2018. Penelitian ini bertujuan untuk mengidentifikasi dampak dan menilai risiko yang ada pada Dinas Perpustakaan dan Kearsipan Kota Salatiga, serta memberikan rekomendasi dan langkah mitigasi sesuai dengan standar ISO 31000:2018. Manfaat dari penelitian ini diharapkan mampu membantu Dinas Perpustakaan dan Kearsipan Kota Salatiga dalam mengidentifikasi dan mengelola risiko yang mungkin timbul, serta menjadi panduan untuk menangani dan mengurangi risiko teknologi informasi di instansi tersebut.

2. METODE

Penyajian penelitian tentang manajemen risiko di Dinas Perpustakaan dan Kearsipan Kota Salatiga menggunakan metode *case study research*. Metode ini hanya berfokus pada satu objek, yaitu aplikasi INLISlite di lembaga tersebut. Selain itu, pendekatan kualitatif digunakan peneliti untuk melakukan observasi lapangan secara langsung untuk mendapatkan informasi dan data yang akurat dan dapat dipertanggungjawabkan.

Pada kasus manajemen risiko pada aplikasi INLISlite di Dinas Perpustakaan dan Kearsipan Kota Salatiga, Framework ISO 31000:2018 digunakan sebagai metodologi

penelitian. Prinsip dan pedoman ISO 31000 sangat tepat digunakan dan diakui secara internasional. Identifikasi risiko, analisis risiko, dan evaluasi risiko digunakan sebagai tahapan dalam penelitian ini (Andika & Wijaya, 2022).



Gambar 1: Proses Manajemen Resiko

Gambar proses manajemen risiko pada gambar 1 menunjukkan bahwa tahapan pertama dalam penilaian risiko untuk aplikasi CUPK Mobile adalah melakukan penelitian risiko menggunakan metode yang sistematis untuk menentukan apakah risiko tersebut dapat diterima atau tidak.

Identifikasi risiko adalah tahap pertama dalam manajemen risiko, yang dilakukan untuk menentukan jenis risiko yang ada dalam suatu organisasi (Sumiyati et al., 2020). Identifikasi risiko adalah proses untuk mengidentifikasi dan mengevaluasi semua faktor risiko yang mungkin terjadi dalam proses operasional binsis perusahaan. Ini dilakukan untuk semua proses binsis yang ada di perusahaan, dengan tujuan untuk mengetahui semua faktor risiko yang mungkin terjadi, termasuk faktor manusia, sistem yang diimplementasikan, dan infrastruktur.

Tahap kedua adalah Analisis Risiko. Analisis risiko mencakup segala sesuatu yang dapat mempengaruhi penilaian, karaterisasi, dan manajemen risiko yang berkaitan dengan infrastruktur SI/TI perusahaan. Peneliti menggunakan Tabel Kriteria Kemungkinan (Likelihood), yang terdiri dari lima kategori: Jarang Sekali (Rare), Jarang Terjadi (Unlikely), Cukup Sering Terjadi (Moderate), Sering Terjadi (Likely) dan Selalu Terjadi (Certain). Tabel ini dapat membantu organisasi dalam mengidentifikasi dan mengelola risiko dengan lebih baik serta memberikan arahan untuk proses pengambilan keputusan terkait pengurangan risiko (Kholifah & Yulhendri, 2024).

Tahap ketiga adalah Evaluasi Risiko (Risk Evaluation). Ini adalah proses penilaian risiko di mana risiko dikelompokkan berdasarkan tingkat risiko, mulai dari risiko terendah hingga risiko tertinggi. Ada tiga tingkat risiko, yaitu rendah (*Low*), sedang (*Medium*), dan tinggi (*High*). Evaluasi risiko dalam mengidentifikasi dan mengelompokkan risiko untuk mendukung pengambilan keputusan yang lebih baik dalam mitigasi risiko penting untuk dilakukan (Geofanny & Tanaamah, 2022). Dalam matriks yang ada, nilai Likehood dan nilai Efek dari proses sebelumnya akan dibedakan kembali dari kemungkinan risiko yang telah ditentukan. Salah satu tujuan dari evaluasi risiko adalah untuk menghasilkan proses pengambilan keputusan terkait risiko yang didasarkan pada hasil analisis risiko. Dalam tahap Perlakuan Risiko (Risk Treatment), satu atau lebih pilihan tindakan akan ditawarkan untuk menangani risiko yang telah diidentifikasi, yang akan memungkinkan penerapan penanganan risiko yang lebih efisien.

Pengumpulan data dilakukan menggunakan pendekatan kualitatif, dengan fokus memahami peristiwa yang dialami oleh subjek dari penelitian ini, seperti perilaku sehari-hari, persepsi dari setiap subjek penelitian, serta tindakan yang dilakukan pada berbagai risiko yang ada dapat dimitigasi. Pendekatan kualitatif memungkinkan peneliti untuk menggali lebih dalam tentang pengalaman dan persepsi seseorang terhadap risiko (Inggrid et al., 2024). Dapat disimpulkan bahwa metode kualitatif berakar pada keseluruhan lingkungan alam, dengan manusia sebagai sumber data yang digunakan penelitiannya. Data primer untuk metode kualitatif adalah hasil dari tanggapan narasumber, dapat dengan wawancara dengan staff TI di Dinas Perpustakaan dan Kearsipan Kota Salatiga.

3. HASIL DAN PEMBAHASAN

Identifikasi Risiko

Tujuan dari tahap identifikasi risiko ini adalah untuk menemukan, mengidentifikasi, dan menjelaskan potensi risiko melalui wawancara. Wawancara dilakukan dengan berbagai sumber yang ahli dalam bidang mereka. Tabel 1 menggambarkan berbagai potensi bahaya.

Tabel 1. Identifikasi Risiko

ID	Faktor	Kemungkinan Risiko
R01	Alam	Gempa bumi
R02		Banjir
R03		Petir
R04		Kebakaran
R05		Listrik padam
R06	Manusia	Penyalahgunaan hak akses
R07		Hacking
R08		Human error
R09		Kurangnya pelatihan
R10	Sistem	Server down
R11		Kapasitas penuh
R12		Overheating
R13		Kehilangan data
R14		Data korup
R15		Versi perangkat lunak yang sudah lama
R16		Web server bermasalah
R17		Backup failure
R18		Koneksi internet terganggu
R19		Kerusakan perangkat
R20		CCTV tidak berfungsi dengan baik

Sumber: Data Primer, diolah (2024)

Setelah mengidentifikasi kemungkinan risiko, ditemukan dua puluh ancaman atau risiko yang berasal dari faktor alam, manusia, dan sistem. Setelah mengidentifikasi kemungkinan risiko, penting untuk mengevaluasi konsekuensi dari setiap ancaman yang telah diidentifikasi.

Tabel 2. Penentuan Dampak Risiko

ID	Faktor	Kemungkinan Risiko	Dampak
R01	Alam	Gempa bumi	Kerusakan fisik pada infrastruktur server dan perangkat dan menghambat proses bisnis
R02		Banjir	Perangkat keras rusak akibat air, kehilangan data serta gnagguan operasional
R03		Petir	Kerusakan perangkat elektronik dan jaringan, menyebabkan downtime serta risiko kehilangan data

ID	Faktor	Kemungkinan Risiko	Dampak
R04		Kebakaran	Proses layanan perpustakaan terganggu
R05		Listrik padam	Kerusakan total pada perangkat keras serta gangguan jangka panjang
R06	Manusia	Penyalahgunaan hak akses	Kebocoran data sensi-tif dan perubahan data
R07		Hacking	Pencurian data serta manipulasi data sensitif
R08		Human error	Kesalahan input data atau penghapusan data yang tidak sengaja, yang dapat mengganggu layanan
R09		Kurangnya pelatihan	Penggunaan sistem yang tidak efisen sehingga mengganggu operasional perpustakaan
R10	Sistem	Server down	Akses ke sistem terhenti yang mengganggu layanan perpustakaan dan keluhan dari pengguna meningkat
R11		Kapasitas penuh	Data tidak dapat tersimpan
R12		Overheating	Kerusakan perangkat keras serta potensi downtime sistem
R13		Kehilangan data	Hilangnya informasi penting yang berdampak pada operasional perpustakaan dan kepuasan pengguna
R14		Data korup	Ketidakakuratan data serta kehilangan data
R15		Versi perangkat lunak yang sudah lama	Sistem rentan terhadap serangan keamanan dan tidak mendukung fitur terbaru
R16		Web server bermasalah	Layanan tidak bisa di akses secara online

ID	Faktor	Kemungkinan Risiko	Dampak
			sehingga menghambat operasional dan pelayanan pengguna
R17		Backup failure	Meningkatkan risiko kehilangan data dan tidak dapat dipulihkan
R18		Koneksi internet terganggu	Pengguna tidak dapat mengakses layanan dan produktivitas pustakawan menurun
R19		Kerusakan perangkat	Perangkat tidak bisa digunakan untuk mendukung operasional
R20		CCTV tidak berfungsi dengan baik	Penurunan pengawasan keamanan, meningkatkan risiko pelanggaran keamanan fisik dan digital

Sumber: Data Primer, diolah (2024)

Setelah mengidentifikasi kemungkinan risiko, ditemukan dua puluh ancaman atau risiko yang berasal dari faktor alam, manusia, dan sistem. Setelah mengidentifikasi kemungkinan risiko, penting untuk mengevaluasi konsekuensi dari setiap ancaman yang telah diidentifikasi.

Analisis Risiko

Analisis risiko adalah bagian dari pemahaman lebih lanjut tentang risiko. Ini berarti menentukan status risiko melalui peringkat frekuensi kejadian. Analisis risiko adalah alat yang dapat digunakan untuk membuat keputusan tentang risiko yang mungkin terjadi. Ada beberapa temuan bahaya yang dikhawatirkan terjadi di DINPERSIP Kota Salatiga. Sehubungan dengan temuan risiko yang sering terjadi, proses bisnis IT yang ada di DINPERSIP Kota Salatiga terganggu.

Tabel 3. Kategori Risiko

Frekuensi	Kategori	Keterangan
1	*Rare*	Kecil kemungkinan terjadi/ tidak pernah terjadi > 2 tahun
2	*Unlikely*	Risiko jarang terjadi 1 – 2 tahun
3	*Moderate*	Risiko terkadang terjadi pada 7 – 12 Bulan
4	*Likely*	Risiko sering terjadi 4 – 6 Bulan
5	*Certain*	Risiko pasti terjadi 1 – 3 Bulan

Sumber: Data Primer, diolah (2024)

Tabel 4. Nilai Risiko

Nilai	Keterangan
Insignificat	Risiko tidak mengganggu aktivitas proses bisnis
Minor	Risiko sedikit menghambat proses bisnis
Moderate	Risiko mengganggu proses bisnis
Major	Risiko menghambat bagian tertentu proses bisnis
Catastrophic	Risiko menghambat serta mengganggu seluruh proses bisnis

Sumber: Data Primer, diolah (2024)

Berikut adalah tabel analisa risiko dengan nilai kemungkinan frekuensi kejadian dan dampak pada masing-masing risiko yang ada.

Tabel 5. Tabel Analisa Risiko

ID	Faktor	Kemungkinan Risiko	Frekuensi	Dampak
R01	Alam	Gempa bumi	1	5
R02		Banjir	3	4
R03		Petir	2	4
R04		Kebakaran	2	5
R05		Listrik padam	3	3
R06		Penyalahgunaan hak akses	2	2
R07		Hacking	2	4
R08	Manusia	Human error	3	3
R09		Kurangnya pelatihan	3	2
R10	Sistem	Server down	3	5
R11		Kapasitas penuh	1	3
R12		Overheating	3	1
R13		Kehilangan data	4	4
R14		Data korup	1	4
R15		Versi perangkat lunak yang sudah lama	4	4
R16		Web server bermasalah	3	5
R17		Backup failure	2	5
R18		Koneksi internet terganggu	3	4
R19		Kerusakan perangkat	3	3
R20		CCTV tidak berfungsi dengan baik	2	2

Sumber: Data Primer, diolah (2024)

Evaluasi Risiko

Pada tahap ini, diperlukan untuk membandingkan hasil analisis risiko dengan standar risiko yang telah ditetapkan sebelumnya. Tahap ini bertujuan untuk menentukan tingkat prioritas risiko yang tinggi atau rendah.

Tabel 6. Matriks Evaluasi Risiko

Frekuensi	**Sangat Sering**	**5**	Medium	Medium	High	High	High
	Sering	**4**	Medium	Medium	Medium	High	High
	Sedang	**3**	Low	Medium	Medium	Medium	High
	Jarang	**2**	Low	Low	Medium	Medium	Medium
	Sangat jarang	**1**	Low	Low	Low	Medium	Medium
Dampak			**1**	**2**	**3**	**4**	**5**
			Sangat ringan	**Ringan**	**Sedang**	**Berat**	**Sangat berat**

Sumber: Data Primer, diolah (2024)

Tabel matrix evaluasi risiko di atas memiliki tiga warna: Merah, Kuning, dan Hijau. Warna Merah menunjukkan level risiko *High*, yang berarti kemungkinan risiko tersebut sering terjadi dan berdampak besar pada aktivitas bisnis organisasi. Warna Kuning menunjukkan level risiko *Medium*, yang berarti kemungkinan risiko tersebut jarang terjadi dan tidak berdampak besar pada aktivitas bisnis organisasi. Warna Hijau menunjukkan level risiko *Low*, yang berarti kemungkinan risiko tersebut jarang terjadi dan berdampak sedikit Selanjutnya, evaluasi risiko dilakukan dengan mengidentifikasi kemungkinan risiko ke dalam parameter menggunakan kriteria kemungkinan dan dampak.

Tabel 7. Kemungkinan Risiko Berdasarkan Tingkatan Level

Frekuensi	**Sangat Sering**	**5**					
	Sering	**4**				R13	R15
	Sedang	**3**	R12	R09	R08 R19 R05	R18	R10 R07
	Jarang	**2**	R20	R06	R02	R03 R16	R04 R17
	Sangat Jarang	**1**			R11	R14	R01
Dampak			**1** **Sangat ringan**	**2** **Ringan**	**3** **Sedang**	**4** **Berat**	**5** **Sangat berat**

Sumber: Data Primer, diolah (2024)

1

Setelah kemungkinan risiko telah dimasukkan ke dalam matrix evaluasi risiko, dua puluh kemungkinan risiko dikelompokkan menurut tingkatan mereka, yang dimulai dengan tingkat tinggi, tingkat tengah, dan tingkat rendah.

Tabel 8. Pengelompokkan risiko Berdasarkan tingkatan level

ID	Kemungkinan Risiko	Frekuensi	Dampak	Level
R15	Versi perangkat yang sudah lama	4	5	High
R13	Kehilangan data	4	4	High
R10	Server down	3	4	High
R07	Hacking	3	5	High
R18	Koneksi Internet terganggu	3	4	Medium
R08	Human error	3	3	Medium
R19	Kerusakan perangkat	3	3	Medium
R05	Listrik padam	3	3	Medium
R09	Kurangnya pelatihan	3	2	Medium
R04	kebakaran	2	5	Medium
R17	Backup failure	2	5	Medium
R03	Petir	2	4	Medium
R16	Web server bermasalah	2	4	Medium
R02	Banjir	2	3	Medium
R01	Gempa bumi	1	5	Medium
R14	Data korup	1	4	Medium
R12	Overheating	3	1	Low
R20	CCTV tidak berfungsi dengan baik	2	2	Low
R06	Penyalahgunaan hak akses	2	2	Low
R11	Kapasistas penuh	1	3	Low

Sumber: Data Primer, diolah (2024)

Setelah kemungkinan risiko telah dimasukkan ke dalam matrix evaluasi risiko, dua puluh kemungkinan risiko dikelompokkan menurut tingkatan mereka, yang dimulai dengan tingkat tinggi, tingkat tengah, dan tingkat rendah.

Perlakuan Risiko

Setelah melewati tahap identifikasi risiko, berikutnya adalah tahap perlakukan risiko. Pada tahap ini, usulan tindakan risiko diberikan untuk setiap kemungkinan risiko. Tujuan dari usulan tindakan risiko ini adalah untuk mengurangi atau meminimalkan semua risiko yang terjadi di sekitar aplikasi INLISlite.

Tabel 9. Tindakan Risiko

ID	Kemungkinan Risiko	Level	Tindakan risiko
R15	Versi perangkat yang lama	High	Mengupgrade php ke versi yang terbaru karena versi terbaru akan memiliki pembaruan keamanan dan peningkatan peforma
R13	Kehilangan data	High	Melakukan backup data secara berkala serta penyimpanan off-site
R10	Server down	High	Melakukan monitoring sistem secara real-time, memastikan adanya server cadangan dan pemeliharaan rutin
R07	Hacking	High	Memasang firewall, enkrisipi data serta melakukan audit keamanan secara berkala
R18	Koneksi internet terganggu	Medium	Memiliki cadangan koneksi internet ISP lain, serta menggunakan load balancer untuk memastikan akses tetap stabil
R08	Human error	Medium	Memberi pelatihan rutin pada staf tentang penggunaan sistem dan pentingnya melakukan penngecekan sebelum menyimpan data
R19	Kerusakan perangkat	Medium	Melakukan pemeliharaan cadangan dan memilik kontrak servis dengan penyedia perangkat
R05	Listrik padam	Medium	Menyediakan genset sebagai sumber daya cadangan yang dapat diaktifkan ketika terjadi pemadaman listrik dalam waktu lama
R09	Kurangnya pelatihan	Medium	Melakukan pelatihan berkala untuk meningkatkan keterampilan staf dalam menggunakan sistem IT perpustakaan
R04	Kebakaran	Medium	Menyediakan alat pemadam kebakaran di setiap ruang dan memasang sensor asap atau alarm

ID	Kemungkinan Risiko	Level	Tindakan risiko
R17	Backup failure	Medium	Menggunakan backup otomatis dan terjadwal, memeriksa integritas backup secara rutin dan menyimpan data backup di lokasi yang terpisah
R03	Petir	Medium	Memasang penangkal petir untuk melindungi perangkat elektronik
R16	Web server bermasalah	Medium	Pemberitahuan kepada pengguna kalau web bermasalah dan melakukan troubleshooting saat web bermasalah
R02	Banjir	Medium	Meletakkan perangkat keras dari tempat yang aman dari banjir
R01	Gempa bumi	Medium	Menyediakan tempat yang aman untuk perangkat
R14	Data korup	Medium	Menjalankan verivikasi data secara berkala, melakukan backup, serta menggunakan checksum unuk memeriksa integritas data
R12	Overheating	Low	Memasang pendingin di ruang server dan memonitor suhu ruangan
R20	CCTV tidak berfungsi dengan baik	Low	Melakukan perawatan cctv secara berkala
R06	Penyalahgunaan hak akses	Low	Memberikan batasan akses pada user
R11	Kapasitas penuh	Low	Menambah kapasitas memori yang lebih besar agar daya tampung nya bisa lebih besar

Sumber: Data Primer, diolah (2024)

4. SIMPULAN

Berdasarkan penelitian yang dilakukan di Dinas perpustakaan dan kearsipan kota Salatiga mengenai manajemen risiko SI/TI menggunakan ISO 31000:2018 yang dijalankan melalui berbagai tahapan-tahapan yang dimulai dari tahapan penilaian risiko (identifikasi risiko, analisis risiko dan evaluasi risiko) hingga tahap perlakuan risiko.

Berdasarkan berbagai tahapan yang sudah dilewati, ditemukan 4 kemungkinan ancaman risiko pada level rendah, 12 kemungkinan ancaman pada level menengah, 4 kemungkinan ancaman pada level tinggi yang tercantum pada tabel ? evlauasi risiko. Dapat disimpulkan bahwa Dinas Perpustakaan dan Kearsipan Kota Salatiga harus mulai menyusun mitigasi dari kemumgkinan risiko yang ada, untuk meminimalisi dan mempersiapkan diri dari ancaman terjadinya risiko pada masa depan. Terutama pada permasalahan versi perangkat yang sudah lama yang saat ini menggunakan PHP 5.6 dimana hal tersebut mengakibatkan rentannnya aplikasi INLISlite sering kali menjadi

sasaran hacker sehingga di beberapa perpustakaan kabupaten kota telah mengalami kehilangan data.

Manajemen risiko di Dinas Perpustakaan dan Kearsipan Kota Salatiga diharapkan dapat perhatian lebih, mengingat ancaman teknologi informasi akan berkembang sejalan dengan berkembangnya teknologi informasi. Dengan harapannya penelitian ini dapat dijadikan acuan pada penyusunan dokumentasi terkait manajemen risiko yang akan datang.

5. DAFTAR PUSTAKA

Agil, M., Sholikhah, N. N., Zunaidi, A., & Ahmada, M. (2023). Meminimalkan risiko dan maksimalkan keuntungan: Strategi manajemen risiko dalam pengelolaan wakaf produktif. *Al-Muraqabah: Journal of Management and Sharia Business*, *3*(2), 1–20.

Aisyah, V. N., Sanjaya, F. P., Usman, I., & Alamsyah, A. I. S. (2024). Evolusi studi tentang risk management dan organisasi: Analisis bibliometrik. *Dialektika: Jurnal Ekonomi Dan Ilmu Sosial*, *9*(1), 13–24.

Amiruddin, Yazid, S., Anggorojati, B., Setiawan, H., Purwoko, R., Kabetta, H., Hadiprakoso, R. B., & Buana, I. K. S. (2023). *Tinjauan strategis keamanan siber Indonesia: Teknologi cloud dan tata kelola data*. Politeknik Siber dan Sandi Negara Press.

Andika, D., & Wijaya, A. (2022). Manajemen risiko teknologi informasi menggunakan framework ISO 31000:2018 pada PT. Trust Lerinvital Timur. *Jurnal Mnemonic*, *5*(2), 111–118. https://doi.org/10.36040/mnemonic.v5i2. 4778

Anita, S. Y., Ketut Tanti Kustina, Wiratikusuma, Y., Sudirjo, F., Sari, D., Nurchayati, Rupiwardani, I., Ruswaji, Nugroho, L., Rakhmawati, I., Harahap, A. K., Anwar, S., Apriani, E., & Sucandrawati, N. L. K. A. S. (2023). *Managemen risiko*. PT Global Eksekutif Teknologi.

Fatmawati, E. (2020). Pengenalan automasi perpustakaan terintegrasi INLISlite. *LIBRARIA: Jurnal Ilmu Perpustakaan Dan Informasi*, *9*(1), 1–19.

Geofanny, G. K., & Tanaamah, A. R. (2022). Sistem manajemen risiko berbasis ISO 31000:2018 di PT. Bawen Mediatama. *JATISI: Jurnal Teknologi Informatika Dan Sistem Informasi*, *9*(4), 2870–2878. https://doi.org/10.35957/ jatisi.v9i4.2484

Hanafi, M. (2021). Manajemen Risiko. In *Risiko, Proses Manajemen Risiko, dan Enterprise Risk Management* (pp. 1–40). Universitas Terbuka.

Harefa, W., & Hartomo, K. D. (2022). Analisis manajemen risiko dengan menggunakan framework ISO 31000:2018 pada sistem informasi gudang. *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(1), 407–420.

Inggrid, Aryaningsih, N. N., & Bagiada, I. M. (2024). Pendekatan kualitatif pengendalian risiko operasional pada sistem pembayaran digital usaha kecil dan

menengah di Kabupaten Badung. *Jurnal Bisnis & Kewirausahaan*, *20*(1), 47–58.

Kholifah, S. N., & Yulhendri. (2024). Analisis manajemen risiko teknologi informasi pada PT Jakarta notebook menggunakan framework ISO 31000. *Scientica: Jurnal Ilmiah Sain Dan Teknologi, 3021–8209*.

Kristiana, R. (2022). *Manajemen risiko: Konsep manajemen risiko*. CV. Mega Press Nusantara.

Pratama, I. P. A. E., & Pratika, M. T. S. (2020). Manajemen risiko teknologi informasi terkait manipulasi dan peretasan sistem pada Bank XYZ tahun 2020 menggunakan ISO 31000:2018. *Jurnal Telematika*, *15*(2).

Royyan, A. (2023). Konsep manajemen risiko. *Jurnal Penelitian Ilmu Ekonomi Dan Keuangan Syariah (JUPIEKES)*, *1*(3), 130–137. https://doi.org/10.59059/jupiekes.v1i3

Sarjana, S. (2020). *Konsep dasar manajemen risiko*. Politeknik Transportasi Darat Indonesia - STTD.

Sarjana, S., Rio Nardo, Hartono, R., Siregar, Z. H., Irmal, Sohilauw, M. I., Wahyuni, S., Rasyid, A., Djaha, Z. A., & Badrianto, Y. (2022). *Managemen risiko*. Media Sains Indonesia.

Sigalingging, S. M., Samar, S., Hasan, I. A., Sukriadi, S., & Nurlin, N. (2024). Peran akuntansi manajemen dalam meningkatkan efisiensi operasional perusahaan. *Jurnal Neraca Peradaban*, *4*(1), 1–6.

Sumiyati, S., Hadiningrum, K., Hazma, H., Susanti, I., & Bakhti, K. Y. (2020). The roles of risk management in achieving organizational Goals. *International Journal of Arts and Social Sciences*, *3*(4), 488–495.

Supriatin, T., & Wijaya, D. P. (2022). Sistem pengadaan bahan pustaka pada dinas arsip dan perpustakaan Kota Bandung. *Visi Pustaka*, *24*(3).

Tabun, M. A., Maria, Sushardi, Hariyani, D. S., Sulistyowati, M., Anwar, Karollah, B., Mariana, Indriani, R., Moonti, A., Nursansiwi, D. A., & Sijabat, F. N. (2023). *Manajemen risiko bisnis era digital (Teori dan pendekatan konseptual)*. Seval Literindo Kreasi.