ANALISIS MANAJEMEN RISIKO MENGGUNAKAN ISO 31000 : 2018 PADA *WEBSITE ACADEMIC INTEGRATED SYSTEM* UNIVERSITAS XYZ

Elfrida Simanjuntak[1], Muhammad Labib Jundillah[2], Vina Zahrotun Kamila[3], Ramadiani Ramadiani[4]

[1,2,3] Program Studi Sistem Informasi, Fakultas Teknik, Universitas Mulawarman, Indonesia
[4] Program Studi Informatika, Fakultas Teknik, Universitas Mulawarman, Indonesia
[1]elfridasmjtk4@gmail.com, [2] muhammadjundillah@ft.unmul.ac.id, [3] vinakamila@ft.unmul.ac.id
[4]ramadiani@unmul.ac.id

Abstrak

Website Academic Integrated System (AIS) Universitas XYZ merupakan sistem yang digunakan untuk mendukung aktivitas administrasi akademik secara daring, seperti pendaftaran mahasiswa baru, pengelolaan kurikulum, pengisian Kartu Rencana Studi (KRS), hingga pengolahan data wisuda. Sistem ini menyimpan berbagai data sensitif mahasiswa, sehingga memiliki potensi risiko yang dapat memengaruhi keamanan dan keberlangsungan layanan. Dalam operasionalnya, AIS menghadapi berbagai risiko seperti perubahan kebijakan Kementerian, *bug* pada fitur KRS, *server down*, serta *human error* yang dapat mengganggu kualitas layanan akademik. Penelitian ini bertujuan untuk menganalisis manajemen risiko pada *Website* AIS menggunakan kerangka kerja ISO 31000:2018. Metode penelitian dilakukan melalui tahapan komunikasi dan konsultasi, penentuan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, serta penentuan perlakuan risiko. Hasil penelitian menunjukkan terdapat 16 risiko yang diklasifikasikan ke dalam tiga kategori, yaitu 3 risiko tinggi (listrik padam, gangguan *Internet Service Provider*, dan *Server Down*), 9 risiko sedang (antara lain Kebakaran, Korsleting Listrik, *Human Error*, *Backup Failure*, *Bug* KRS, *Overload*, dan Update Gagal), serta 4 risiko rendah (Pencurian Hardware, Akses Data Ilegal, Kerusakan Hardware, dan Ketidaksesuaian Sistem Dengan Peraturan Baru). Hasil penelitian ini menunjukkan bahwa penerapan ISO 31000:2018 dapat membantu dalam proses identifikasi, evaluasi, dan penentuan perlakuan risiko pada sistem AIS, sehingga mendukung peningkatan keandalan dan keamanan layanan akademik.

Kata kunci: manajemen risiko, ISO 31000, *academic integrated system*

1. Pendahuluan

Universitas XYZ merupakan salah satu Perguruan Tinggi Negeri (PTN) di Samarinda, Kalimantan Timur, yang memanfaatkan teknologi informasi dalam mendukung kegiatan akademik. Salah satu bentuk pemanfaatannya adalah Website Academic Integrated System (AIS), yang digunakan untuk mempermudah berbagai aktivitas administrasi akademik secara daring, mulai dari pendaftaran mahasiswa baru, pengelolaan kurikulum, Kartu Rencana Studi (KRS), hingga data wisuda (FKM UNMUL, 2023). Keberadaan sistem ini menjadi krusial karena mendukung kelancaran layanan akademik secara menyeluruh.

Secara umum, sistem informasi dapat menghadapi berbagai risiko seperti ketidakstabilan koneksi internet, gangguan listrik, pemeliharaan tidak terencana, kesalahan pengguna, maupun kerusakan infrastruktur (Herlambang et al., 2024). Risiko-risiko serupa juga berpotensi dialami oleh AIS Universitas XYZ. Berdasarkan wawancara dengan Kepala UPA.TIK (Unit Penunjang Akademik Teknologi Informasi dan Komunikasi), AIS dapat berjalan optimal apabila sistem stabil, responsif, dan mampu menangani beban kerja tinggi. Namun, dalam implementasinya, AIS masih menghadapi berbagai kendala seperti kesalahan pengguna (human error), bug pada fitur KRS, serta penyesuaian mendadak terhadap kebijakan kementerian. Selain itu, sistem AIS juga menyimpan data sensitif mahasiswa, sehingga aspek keamanan informasi menjadi hal yang sangat penting. Kondisi ini menunjukkan adanya risiko yang berpotensi mengganggu kelancaran layanan akademik dan perlu dikelola secara sistematis.

Risiko merupakan kejadian yang dapat memengaruhi efektivitas dan efisiensi proses dalam suatu organisasi (Wibowo, 2022). Oleh karena itu, diperlukan pemahaman terhadap risiko agar organisasi dapat meminimalkan dampak negatif yang mungkin terjadi (Salim & Prasetyo, 2023). Manajemen risiko menjadi salah satu pendekatan yang digunakan untuk mengantisipasi potensi risiko di masa depan serta meningkatkan kinerja organisasi melalui pengelolaan sumber daya yang lebih optimal (Muhammad Asir et al., 2023). Selain itu, manajemen risiko juga berperan dalam menciptakan dan menjaga

nilai organisasi melalui peningkatan kinerja dan pencapaian tujuan (Salim & Prasetyo, 2023).

Salah satu kerangka kerja yang dapat digunakan dalam manajemen risiko adalah ISO 31000:2018, yaitu standar yang memberikan panduan dalam menetapkan prinsip, kerangka kerja, serta proses pengelolaan Risiko (Sitanggang & Sitanggang, 2022). Standar ini bersifat fleksibel sehingga dapat diterapkan pada berbagai organisasi dengan tingkat kompleksitas yang berbeda (Izzudin et al., 2024). ISO 31000 pertama kali diterbitkan pada tahun 2009 dan kemudian direvisi pada tahun 2018 oleh organisasi internasional standardisasi untuk menyempurnakan prinsip dan pedoman manajemen risiko (Mukhtar Syafii, 2022). Berdasarkan kondisi yang ada, AIS Universitas XYZ belum menerapkan manajemen risiko berbasis ISO 31000:2018, sehingga diperlukan penerapan kerangka kerja ini untuk mengantisipasi berbagai risiko, baik yang berasal dari faktor teknis maupun non-teknis.

Penelitian sebelumnya oleh Harefa & Hartomo (2022) menunjukkan bahwa penerapan ISO 31000:2018 dapat membantu mengidentifikasi dan mengelola risiko secara sistematis pada sistem informasi. Namun, penelitian tersebut masih berfokus pada sistem informasi umum dan belum mempertimbangkan karakteristik sistem akademik yang memiliki pola penggunaan fluktuatif serta dipengaruhi oleh kebijakan institusi. Oleh karena itu, penelitian ini berfokus pada analisis risiko pada Website Academic Integrated System (AIS) Universitas XYZ.

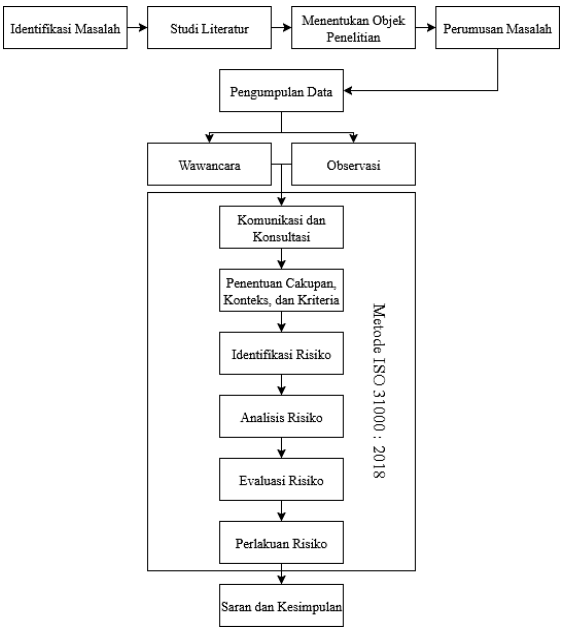
Berdasarkan hal tersebut, penelitian ini berfokus pada analisis manajemen risiko menggunakan kerangka kerja ISO 31000:2018 terhadap Website Academic Integrated System (AIS) Universitas XYZ. Data diperoleh melalui wawancara dengan tiga orang pengelola AIS, yang kemudian dipadukan dengan hasil observasi sistem untuk memperoleh gambaran risiko yang lebih komprehensif. Lingkup penelitian ini mencakup seluruh tahapan manajemen risiko, mulai dari identifikasi, analisis, evaluasi, hingga tahap pemberian rekomendasi perlakuan risiko.

Penelitian ini bertujuan untuk mengidentifikasi risiko yang telah terjadi maupun yang berpotensi terjadi pada sistem AIS, serta menganalisis dampak dari masing-masing risiko terhadap keberlangsungan layanan akademik. Selanjutnya, penelitian ini juga menyusun rekomendasi perlakuan risiko yang bersifat kontekstual dan dapat disesuaikan dengan kondisi operasional sistem di lingkungan Universitas XYZ, sehingga diharapkan dapat menjadi acuan dalam pengelolaan risiko yang lebih terstruktur. Penelitian ini memberikan kontribusi aplikatif melalui (1) pemetaan risiko pada sistem AIS, (2) klasifikasi risiko berdasarkan tingkat kemungkinan dan dampaknya, serta (3) penyusunan rekomendasi mitigasi risiko yang disesuaikan dengan karakteristik operasional sistem AIS. Selain itu, penelitian ini juga diharapkan dapat memberikan gambaran praktis mengenai penerapan ISO 31000:2018 pada sistem informasi akademik yang memiliki karakteristik penggunaan dinamis.

Kebaruan penelitian ini terletak pada analisis risiko pada sistem AIS yang memiliki pola penggunaan fluktuatif, khususnya pada periode kritis seperti pengisian Kartu Rencana Studi (KRS), yang menyebabkan variasi tingkat beban sistem secara signifikan. Selain itu, penelitian ini juga mempertimbangkan faktor non-teknis seperti kebijakan akademik dan perilaku pengguna yang turut memengaruhi tingkat risiko, sehingga memberikan sudut pandang yang lebih komprehensif dibandingkan penelitian sebelumnya.

2. Metode

Tahapan penelitian dimulai dari identifikasi masalah hingga penarikan Kesimpulan. Data hasil wawancara dan observasi, lalu dianalisis menggunakan metode ISO 31000:2018 yang meliputi identifikasi, analisis, evaluasi, dan perlakuan risiko. Tahapan Penelitian dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

Penelitian ini memberikan kontribusi bagi ilmu pengetahuan melalui pemanfaatan ISO 31000 dalam manajemen risiko yang dapat dijadikan referensi bagi penelitian selanjutnya, sekaligus memperkaya kajian sistem informasi melalui penerapan standar tersebut pada analisis risiko *Website* AIS Universitas XYZ sebagai panduan peningkatan keamanan dan keandalannya. Selain itu, penelitian ini juga berkontribusi secara praktis dalam bidang operasional, di mana rekomendasi perlakuan risiko yang dihasilkan dapat membantu meningkatkan keandalan AIS, meminimalkan potensi kerugian akibat risiko yang tidak terkelola, serta mendukung keberlanjutan operasional dan pencapaian tujuan

jangka panjang universitas dalam menyediakan layanan administrasi akademik secara online.

Keterbaruan penelitian ini terletak pada objek yang diteliti, yaitu *website Academic Integrated System* Universitas XYZ, yang belum pernah menjadi fokus dalam penelitian sebelumnya. Selain itu, keterbaruan juga terletak pada jenis narasumber yang dilibatkan. Narasumber yang dilibatkan terdiri dari berbagai latar belakang peran dan tanggungjawab, yaitu Kepala IT, *Developer*, serta Admin.

2.1. Identifikasi Masalah

Tahap identifikasi masalah dilakukan untuk menemukan permasalahan utama yang akan diteliti. Permasalahan yang teridentifikasi selanjutnya menjadi dasar untuk melakukan kajian lebih mendalam.

2.2. Studi Literatur

Studi literatur bertujuan untuk memperluas dan memperdalam pemahaman terhadap permasalahan yang diangkat dalam penelitian. Penelitian ini memperolah informasi dari berbagai sumber seperti buku, jurnal, artikel ilmiah, dan halaman web, dengan rentang tahun terbitan antara 2021 hingga 2025. Dengan mempelajari sumber-sumber tersebut, peneliti dapat memperoleh wawasan yang lebih mendalam mengenai masalah dalam penelitian, serta menemukan teori yang mendukung penelitian.

2.3. Penentuan Objek Penelitian

Berdasarkan hasil observasi langsung, diperoleh informasi bahwa AIS belum mengadopsi manajemen risiko berbasis ISO 31000:2018. Oleh karena itu, *website* AIS Universitas XYZ ditetapkan sebagai objek penelitian.

2.4. Perumusan Masalah

Rumusan masalah dapat katakan seperti pertanyaan yang jawabannya merupakan hasil dari penelitian. Identifikasi masalah dan studi literatur yang menjadi fokus penelitian diperlukan untuk melakukan perumusan masalah. Perumusan masalah berperan penting dalam mempersempit batasan penelitian, sehingga fokus penelitian menjadi lebih spesifik.

2.5. Pengumpulan Data

1. Wawancara

   Wawancara dilakukan untuk memperoleh data dan informasi dibutuhkan seperti data aset, jenis risiko yang pernah terjadi serta berpontensi terjadi, dan dampak dari risiko tersebut. Wawancara dilakukan terhadap narasumber yang sudah ditentukan menggunakan RACI *Matrix. RACI Matrix* dipakai untuk mengidentifikasi dan menetapkan pihak-pihak yang akan menjadi narasumber sesuai peran masing-masing (Rahayu et al., 2024). Sesuai dengan namanya RACI terdiri dari empat elemen yang masing-masing merepresentasikan jenis peran dan tanggung jawab yang berbeda dalam suatu proses atau proyek organisasi (Wirayudha et al., 2024), yaitu:

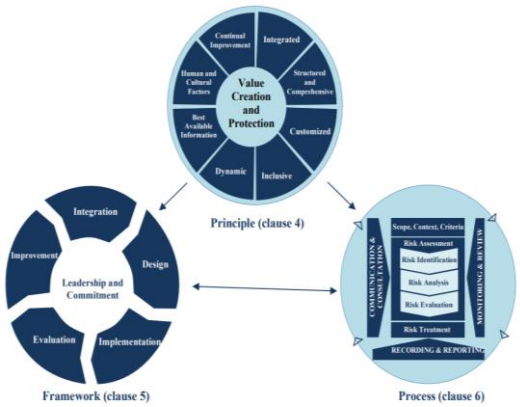
   1. *Responsible* (R), Siapa yang melaksanakan pekerjaan dan bertanggung jawab secara langsung terhadap pelaksanaan suatu tugas atau pekerjaan.
   2. *Accountable* (A), orang yang memiliki otoritas penuh dalam pengambilan keputusan.
   3. *Consulted* (C), orang yang perlu dikonsultasikan untuk memberikan masukan atau saran.
   4. *Informed* (A), orang yang perlu diinformasikan tentang hasil atau informasi terkait perkembangan proses suatu tugas atau pekerjaan.

2. Observasi

   Observasi dilakukan untuk memperoleh pemahaman secara langsung mengenai berbagai aspek penting terkait objek penelitian. Hasil observasi memberikan gambaran mengenai cakupan permasalahan yang ada pada pengelolaan *website*, serta membantu dalam penentuan konteks internal dan eksternal. Dengan demikian, observasi berperan sebagai dasar dalam tahapan selanjutnya pada implementasi ISO 31000 : 2018, khususnya pada penentuan cakupan, konteks, dan kriteria.

2.6. Penerapan Metode ISO 31000 : 2018

ISO 31000:2018 adalah standar manajemen risiko dalam organisasi atau perusahaan yang berfungsi untuk menetapkan dasar dan kerangka kerja melalui program manajemen risiko (Sitanggang & Sitanggang, 2022). Menurut (Harefa & Hartomo, 2022) penilaian risiko menggunakan metode ISO 31000:2018 terdiri dari tiga tahapan, yaitu Identifikasi Risik, Analisis Risiko, dan Evaluasi Risiko. ISO 31000:2018 didasarkan pada 3 elemen, yaitu: prinsip, kerangka kerja, dan proses manajemen risiko. ISO 31000:2018 dapat dilihat pada Gambar 2.



Gambar 2. Kriteria *Impact*

1. Komunikasi dan Konsultasi

   Pengumpulan data dilakukan melalui wawancara, masing-masing narasumber memiliki peran yang berbeda sesuai dengan tugas dan tanggung jawabnya masing - masing. Narasumber yang dipilih, yaitu :

   1. Hidayat Muttaqien sebagai Kepala UPA.TIK yang menjadi narasumber 1 (N1)
   2. Nur Fauzan Hidayat sebagai *Developer* AIS yang menjadi narasumber 2 (N2)
   3. Isay Mangele sebagai Admin AIS yang menjadi narasumber 3 (N3).

   Keterlibatan ketiga narasumber tersebut dalam memberikan informasi ditentukan menggunakan RACI Matrix, sebagaimana ditampilkan pada Tabel 1. Matriks ini membantu menggambarkan peran dan tingkat keterlibatan setiap narasumber secara lebih jelas.

Tabel 1. RACI Matrix

No	Aktivitas	N1	N2	N3
1	Memberikan informasi terkait aset data, aset *software*, dan aset *hardware*	A	R	R
2	Memberikan informasi terkait risiko maupun kemungkinan risiko beserta dampaknya	A	R	R
3	Memberikan nilai *Likelihood* dan nilai *Impact* terhadap risiko maupun kemungkinan risiko	A	R	R
4	Konsultasi mengenai rekomendasi perlakuan risiko sebagai hasil akhir	C/A	C	C

2. Penentuan cakupan, konteks, dan kriteria

   Cakupan pada penelitian ini meliputi kegiatan wawancara yang dilakukan terhadap tiga orang pengelola *website* AIS. Fokus penelitian ini tertuju pada *website* AIS yang digunakan di Universitas XYZ. Penelitian ini mencakup tahapan komunikasi dan konsultasi, penentuan cakupan, konteks, dan kriteria, identifikasi risiko, identifikasi kemungkinan dan dampak yang ditimbulkan, evaluasi risiko, serta rekomendasi perlakuan risiko.

   Konteks dari website AIS adalah sebagai sarana pendukung aktivitas akademik, seperti proses pendaftaran mahasiswa, pengelolaan data kurikulum, serta penyimpanan data sensitif mahasiswa. Dalam pelaksanaannya, sistem ini menghadapi sejumlah tantangan, seperti gangguan teknis, kesalahan penggunaan, serta perubahan kebijakan dari kementerian. Selain itu, aspek keamanan data menjadi perhatian utama karena data yang dikelola bersifat penting dan rahasia. Kondisi ini menjadi semakin kompleks karena AIS Universitas XYZ dikelola oleh tim internal dengan beban layanan yang sangat tinggi pada periode tertentu, seperti pengisian KRS dan pendaftaran wisuda, sehingga pola risikonya berbeda dari perguruan tinggi lain. Risiko-risiko yang ditemukan berdasarkan wawancara juga menunjukkan karakteristik khusus AIS Unmul, seperti bug modul KRS dan ketidaksesuaian sistem akibat perubahan mendadak kebijakan akademik. Hal inilah yang membentuk konteks risiko yang unik pada AIS dibandingkan sistem akademik serupa di perguruan tinggi lainnya.

   Kriteria yang digunakan dalam penelitian ini mencakup pembagian identifikasi risiko ke dalam tiga faktor, yaitu faktor lingkungan, faktor manusia, serta faktor sistem dan infrastruktur.

3. Identifikasi Risiko

   Tahapan identifikasi risiko mencakup identifikasi aset, identifikasi risiko, serta identifikasi dampak risiko. Aset yang akan diidentifikasi berupa aset data, aset *software*, serta aset .

4. Analisis Risiko

   Analisis risiko dilakukan menggunakan nilai kriteria *likelihood* (kemungkinan) dan nilai kriteria *impact* (dampak). Analisis risiko *likelihood* dilakukan dengan cara memberikan nilai pada setiap risiko yang telah diidentifikasi berdasarkan kemungkinan terjadinya risiko dalam periode waktu tertentu. Kriteria *likelihood* dapat dilihat pada Tabel 2.

Tabel 2. Kriteria *Likelihood*

Likelihood		Keterangan	Frekuensi Kejadian
Nilai	Kriteria		
1	*Rare*	Risiko yang hampir tidak pernah terjadi	> 2 Tahun
2	*Unlikely*	Risiko yang jarang terjadi	1- 2 Tahun
3	*Possible*	Risiko yang kadang terjadi	1- 2 Tahun
4	*Likely*	Risiko yang sering terjadi	4 - 6 Bulan
5	*Certain*	Risiko yang pasti terjadi	4 - 6 Bulan

Analisis risiko impact dilakukan dengan memberikan nilai pada setiap risiko yang telah diidentifikasi, dengan mempertimbangkan tingkat dampak yang ditimbulkan serta sejauh mana risiko tersebut dapat memengaruhi jalannya proses bisnis secara keseluruhan. Penilaian ini bertujuan untuk mengetahui prioritas penanganan risiko, sehingga organisasi dapat lebih fokus dalam mengelola risiko yang memiliki dampak paling signifikan terhadap operasional. Selain itu, analisis ini juga membantu dalam mengantisipasi potensi kerugian yang mungkin terjadi, baik dari segi finansial, reputasi, maupun keberlangsungan bisnis. Kriteria impact yang digunakan sebagai

acuan dalam proses penilaian ini dapat dilihat pada Tabel 3.

Tabel 3. Kriteria *Impact*

Nilai	*Impact* Kriteria	Keterangan
1	*Insignificant*	Risiko yang tidak terlalu mengganggu proses bisnis pada w*ebsite* AIS
2	*Minor*	Risiko yang sedikit menghambat aktifitas namun tidak mengganggu proses bisnis pada *website* AIS
3	*Moderate*	Risiko yang menghambat sebagian proses bisnis pada *website* AIS
4	*Major*	Risiko yang menghambat hampir seluruh proses bisnis pada *website* AIS
5	*Catastrophic*	Risiko yang menghambat seluruh proses bisnis pada *website* AIS

Nilai dari hasil analisis *Likelihood* dan *Impact* kemudian akan dihitung nilai rata-ratanya dengan menggunakan persamaan 1.

$$\overline{\mathcal{X}} = \frac{\sum_{i=1}^{n} x_i}{n} \quad (1)$$

Diketahui,
$\overline{\mathcal{X}}$ = Rata-rata
Σ = Penjumlahan
n = jumlah keseluruhan data
x_i = nilai data ke-i

5. Evaluasi Risiko

Evaluasi risiko dilakukan menempatkan risiko- risiko yang telah dianalisis ke dalam *matrix* evaluasi berdasarkan nilai *likelihood* dan nilai *impact.* Evaluasi risiko dilakukan sebagai upaya untuk mendapatkan risiko yang mempunyai dampak *level* rendah (*Low)*, menengah (*Medium*), dan tinggi (*High*. Semakin ke kanan, dampak yang ditimbulkan oleh risiko semakin besar, sedangkan semakin ke bawah, kemungkinan terjadinya risiko semakin tinggi. Dengan demikian, posisi setiap risiko dalam *matrix* ditentukan berdasarkan titik perpotongan antara nilai *likelihood* dan nilai *impact*. Titik perpotongan ini merupakan level dari risiko yang dievaluasi. Warna hijau menunjukkan *level* risiko rendah, warna kuning menunjukkan *level* risiko sedang, dan warna merah menunjukkan *level* risiko tinggi. Lalu, risiko-risiko kemudian akan dikelompokkan berdasarkan hasil evaluasi risiko. M*atrix* evaluasi risiko dapat dilihat pada Tabel 4.

Tabel 4. Matrix Evaluasi Risiko

	Likelihood				
Impact	**Rare (1)**	**Unlikely (2)**	**Possible (3)**	**Likely (4)**	**Certain (5)**
1 *Insignificant*	*Low*	*Low*	*Low*	*Medium*	*Medium*
2 *Minor*	*Low*	*Low*	*Medium*	*Medium*	*Medium*
3 *Moderate*	*Low*	*Medium*	*Medium*	*Medium*	*High*
4 *Major*	*Medium*	*Medium*	*Medium*	*High*	*High*
5 *Catastrophic*	*Medium*	*Medium*	*High*	*High*	*High*

6. Perlakuan Risiko

Rekomendasi perlakuan risiko akan disusun berdasarkan *Level* risiko. Rekomendasi perlakuan akan dikonsultasikan dengan pihak terkait untuk mengetahui rekomendasi yang dapat diterima ataupun belum dapat diterima, risiko mana saja yang telah diterapkan maupun yang belum diterapkan, serta untuk mengetahui kendala yang menyebabkan rekomendasi tersebut belum dapat diterapkan ataupun diterima.

3. Hasil Analisis

3.1. Identifikasi Risiko

Tahapan identifikasi risiko mencakup 3 langkah, yaitu identifikasi aset, identifikasi risiko, serta identifikasi dampak risiko.

1. Identifikasi Aset

Aset yang diidentifikasi terdiri dari tiga kategori yang meliputi aset data, aset software, dan aset *Hardware.* Daftar aset dapat dilihat pada Tabel 5.

Tabel 5. Identifikasi Aset

Kategori Aset	Nama Aset
Data	1. Data Mahasiswa
	2. Data Dosen
Software	1. *Website Academic Integrated System* (AIS)
	2. PHP
	3. Ci4
	4. Nginx
	5. Oracle
	6. Linux
Hardware	1. Komputer
	2. Monitor
	3. Server

2. Identifikasi Risiko

Identifikasi risiko dilakukan dengan mengelompokkan risiko menjadi tiga faktor penyebab, yaitu lingkungan, manusia, serta teknologi dan infrastruktur, yang dapat dilihat pada Tabel 6.

Tabel 6. Identifikasi Risiko

Faktor	ID	Risiko
Lingkungan	R01	Listrik Padam
	R02	Petir
	R03	Korsleting listrik
	R04	Kebakaran
	R05	Gangguan *Internet Service Provider* (ISP)
Manusia	R06	*Human Error* (Kesalahan Pengguna)
	R07	Data dan Informasi dilihat oleh pihak yang tidak berwenang
	R08	Pencurian *Hardware*
	R09	*Serverdown*

Faktor	ID	Risiko
Sistem dan Infrastruktur	R10	*Backup Failure* (proses penyimpanan data gagal)
	R11	Ketidaksesuaian Sistem dengan Peraturan Baru
	R12	*Bug* fitur KRS
	R13	*Overload*
	R14	Kerusakan *Hardware*
	R15	*Update* Gagal
	R16	*Error* pada fitur tertentu

3. Identifikasi Dampak Risiko

Tahap identifikasi dampak risiko ini bertujuan untuk mengetahui apa saja dampak yang mungkin terjadi ataupun yang sudah terjadi dari risiko yang bisa berdampak pada keberlangsungan *website* AIS. Hasil Identifikasi Dampak Risiko dapat dilihat pada Tabel 7.

Tabel 7. Identifikasi Risiko

ID	Risiko	Dampak
R01	Listrik Padam	AIS tidak dapat diakses.
R02	Petir	Terjadi kerusakan pada aset dan infrastruktur. Serta berpotensi dapat menyebabkan kebakaran.
R03	Kebakaran	Terjadi kerusakan pada aset.
R04	Korsleting listrik	Terbakarnya peralatan elektronik dan menyebabkan lonjakan daya Listrik secara mendadak yang dapat menyebabkan kerusakan pada perangkat keras.
R05	Gangguan ISP	AIS tidak dapat diakses.
R06	*Human Error*	Ketidakakuratan data mahasiswa yang sebenarnya dengan data yang ada di dalam *website* AIS.
R07	Data diakses oleh pihak yang tidak berwenang	Beberapa informasi yang semestinya terbatas dapat dilihat oleh pihak yang tidak berwenang dan berpotensi data disalahgunakan
R08	Pencurian *Hardware*	Kehilangan *Hardware.*
R09	*Serverdown*	AIS tidak dapat diakses.
R10	*Backup Failure*	Kehilangan data.
R11	Ketidaksesuaian Sistem dengan Peraturan Baru	AIS mengalami penyesuaian dan beberapa proses mengalami perubahan.
R12	*Bug* pada fitur KRS	Menyebabkan jumlah SKS yang ditampilkan pada halaman sistem tidak sesuai dengan jumlah SKS sebenarnya.
R13	*Overload*	*Website* akan lambat dalam melakukan suatu proses permintaan pengguna.
R14	Kerusakan *Hardware*	Dapat menyebabkan gangguan terhadap fungsi *software* yang memerlukan *Hardware* untuk beroperasi.
R15	*Update* Gagal	Fitur baru tidak bisa digunakan.
R16	*Error* pada fitur tertentu	Pengguna tidak dapat mengakses fitur yang *error.*

Risiko pada AIS berdampak pada tiga jenis aset, yaitu hardware, software, dan data. Risiko lingkungan seperti listrik padam, petir, korsleting listrik, kebakaran, dan gangguan ISP (R01–R05) memberi pengaruh langsung pada hardware karena berhubungan dengan kerusakan server dan perangkat jaringan. Risiko tersebut juga memengaruhi software karena AIS tidak dapat beroperasi ketika perangkat fisik tidak berfungsi.

Dampak terhadap data muncul ketika kerusakan terjadi pada saat proses penyimpanan atau ketika perangkat penyimpanan terganggu. Risiko manusia (R06–R08) terutama berpengaruh pada data karena kesalahan input, akses tidak sah, dan ancaman kehilangan data akibat pencurian perangkat.

Risiko pada sistem dan infrastruktur (R09–R16) mengarah pada gangguan software, termasuk server yang tidak merespons, proses backup yang gagal, ketidaksesuaian sistem dengan regulasi baru, bug pada fitur tertentu, beban akses yang melebihi kapasitas, kerusakan perangkat, kegagalan update, dan error pada modul tertentu. Risiko tersebut berpotensi mengganggu keakuratan data, ketersediaan layanan, serta stabilitas perangkat keras.

3.2 Analisis Risiko

Analisis risiko dilakukan berdasarkan kriteria *likelihood* dan kriteria *impact.* Nilai kriteria *likelihood* ditentukan berdasarkan kemungkinan terjadinya suatu risiko dalam periode tertentu. Penilaian *Likelihood* dapat dilihat pada Tabel 8.

Tabel 8. Nilai *Likelihood*

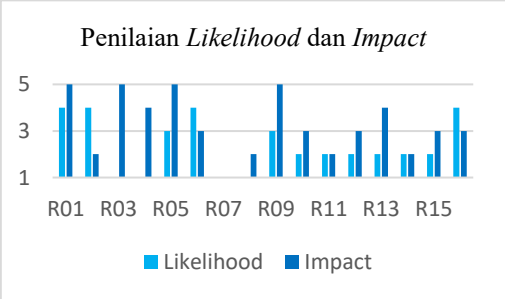
ID	Risiko	*Likelihood*	
		N1	N2
R01	Listrik Padam	4	3
R02	Petir	4	3
R03	Kebakaran	1	1
R04	Korsleting listrik	1	1
R05	Gangguan ISP	4	1
R06	*Human Error*	3	4
R07	Data dilihat oleh pihak yang tidak berwenang	1	1
R08	Pencurian *Hardware*	1	1
R09	*Serverdown*	4	2
R10	*Backup Failure*	2	1
R11	Ketidaksesuaian Sistem dengan Peraturan Baru	3	1
R12	*Bug* pada fitur KRS	2	1
R13	*Overload*	2	1
R14	Kerusakan *Hardware*	2	1
R15	*Update* Gagal	2	2
R16	*Error* pada fitur tertentu	4	3

Nilai kriteria *impact* ditentukan berdasarkan tingkat dampak risiko memengaruhi operasional *website* AIS. Penilaian *Likelihood* dapat dilihat pada Tabel 9.

Tabel 9. Nilai *Impact*

ID	Risiko	*Impact*	
		N1	N2
R01	Listrik Padam	5	5
R02	Petir	1	2
R03	Kebakaran	5	5
R04	Korsleting listrik	3	5
R05	Gangguan ISP	5	5
R06	*Human Error*	2	3
R07	Data dilihat oleh pihak yang tidak berwenang	1	1
R08	Pencurian *Hardware*	2	2
R09	*Serverdown*	5	5
R10	*Backup Failure*	3	2
R11	Ketidaksesuaian Sistem dengan Peraturan Baru	2	2
R12	*Bug* pada fitur KRS	3	2
R13	*Overload*	4	3
R14	Kerusakan *Hardware*	2	2
R15	*Update* Gagal	2	3
R16	*Error* pada fitur tertentu	4	2

Nilai *Likelihood* dan *Impact* dari N1 dan N2, kemudian dihitung nilai rata-ratanya untuk mendapatkan satu nilai dari masing-masing kriteria. Perhitungan rata-rata dilakukan dengan menggunakan Persamaan 2.1. Hal ini berfungsi untuk menyatukan perbedaan penilaian antar kedua narasumber menjadi satu nilai yang lebih objektif. Hasil dari perhitungan nilai *Lilkelihood* dan *Impact* dapat dilihat dalam Gambar 3.



Gambar 3. Diagram Penilaian *Likelihood* dan *Impact*

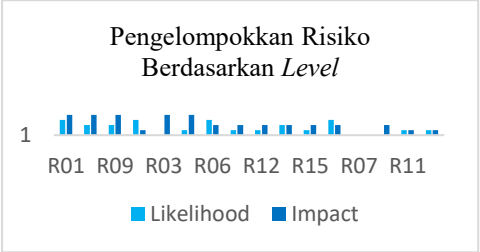
3.3 Evaluasi Risiko

Tahap evaluasi risiko menempatkan risiko yang telah dianalisis ke dalam *matrix* evaluasi berdasarkan nilai *likelihood* dan nilai *impact.* Tahap Evaluasi risiko dilakukan sebagai upaya untuk mendapatkan risiko yang mempunyai dampak paling tinggi, menengah, dan rendah. *Matrix* evaluasi risiko dapat dilihat pada Tabel 10.

Tabel 10. *Matrix* Evaluasi Risiko

Impact	Likelihood				
	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Certain (5)
1 *Insignificant*					
2 *Minor*		R02	R06 R16		R01
3 *Moderate*					R05 R09
4 Major			R11 R14	R10 R12 R15	R13
5 Catastrophic	R07	R08		R04	R03

Hasil dari evaluasi risiko, selanjutnya dikelompokkan ke dalam tiga kategori *Level*, yaitu tinggi, menengah, dan rendah. Pengelompokan ini dilakukan untuk memudahkan penentuan prioritas penanganan risiko sehingga sumber daya dapat digunakan lebih efisien. Pengelompokkan Risiko Berdasarkan *Level* dapat dilihat pada Gambar 4.



Gambar 4. Diagram Pengelompokkan Risiko Berdasarkan Level

3.4 Perlakuan Risiko

Berdasarkan hasil analisis terdapat 16 risiko yang berpotensi memengaruhi keberlangsungan dan kinerja *website*. Maka, diperlukan perlakuan risiko yang dapat mencegah atau mengurangi dampak kerugian akibat risiko tersebut. Keterangan (K) merupakan sebagai penanda singkat untuk jenis perlakuan risiko yang diterapkan. Huruf yang digunakan mewakili empat kategori perlakuan risiko, yaitu **A** untuk *Avoid*, **M** untuk *Mitigate*, **T** untuk *Transfer*, dan **C** untuk *Accept*Rekomendasi perlakuan risiko dapat dilihat pada Tabel 11.

Tabel 11. Rekomendasi Perlakuan Risiko

ID	Risiko	Perlakuan Risiko	K
R01	Listrik Padam	1. Menyediakan *Uninterruptible Power Supply* (UPS). 2. Melakukan pemeriksaan secara berkala terhadap perangkat cadangan listik.	M
R05	Gangguan ISP	Memasang lebih dari satu ISP.	
R09	*Serverdown*	1. Melakukan pemeriksaan secara rutin terhadap database. 2. Melakukan pengecekan rutin pada infrastruktur TI.	M
R02	Petir	Melakukan pemeriksaan secara berkala terhadap alat penangkal petir.	
R03	Kebakaran	Menyediakan *Automatic Fire Suppression System.*	
R04	Korsleting Listrik	Memasang *Miniature/Molded Case*	

ID	Risiko	Perlakuan Risiko	K
		Circuit Breaker (MCB/MCCB).	
R06	*Human Error*	1. Memberi pelatihan terhadap karyawan secara berkala. 2. Mengevaluasi aktivitas pengguna secara berkala.	M
R10	*Backup Failure*	1. Melakukan pemeriksaan secara berkala terhadap penyimpanan. 2. Membuat Otomatisasi *backup*	M M
R12	*Bug* pada fitur KRS	1. Melakukan pengujian (*Testing*) pada setiap fitur. 2. Sediakan fitur pelaporan *bug* atau *feedback* dari pengguna.	M
R13	*Overload*	1. Peningkatan Skalabilitas Otomatis (*Autoscaling*). 2. Peningkatan *Bandwidth* sementara.	M
R15	*Update* Gagal	1. Selalu uji coba di lingkungan *staging.* 2. Merilis fitur baru secara perlahan.	M
R16	*Error* pada fitur tertentu	1. Melakukan pengujian pada setiap fitur. 2. Sediakan fitur pelaporan *bug*	M
R07	Data dilihat oleh pihak yang tidak berwenang	Monitor aktivitas *login* pengguna secara berkala untuk mendeteksi akses tidak sah.	M
R08	Pencurian *Hardware*	1. Gunakan kunci pintu digital/kartu akses. 2. Orang berwenang yang diperbolehkan mengakses ruangan tempat *hardware.*	M
R11	Ketidaksesuaian Sistem dengan peraturan baru	Melakukan perbaikan hanya pada sistem yang memerlukan perubahan supaya tidak menganggu . aktivitas proses bisnis secara keseluruhan pada AIS.	A M
R14	Kerusakan *Hardware*	1. Melakukan pemeriksaan rutin terhadap *hardware.* 2. Menghindari penggunaan *hardware* yang sudah usang atau tidak sesuai kebutuhan operasional.	M

Risiko ini memerlukan perlakuan berupa tindakan *mitigate* karena ketiganya dapat mengganggu layanan inti secara langsung. Ketiga risiko ini dikategorikan *tinggi* karena meskipun tidak selalu terjadi setiap saat, dampaknya sangat besar terhadap kelangsungan operasional *website* AIS. Jika listrik padam, ISP terganggu, atau server mengalami *down*, maka seluruh layanan tidak dapat diakses pengguna, sehingga berpengaruh langsung terhadap keberlangsungan sistem.

Risiko dengan kategori tinggi terdiri dari R01 (listrik padam), R05 (gangguan Internet Service Provider/ISP), dan R09 (server down). Ketiga risiko ini dikategorikan tinggi karena memiliki dampak langsung terhadap terhentinya layanan website AIS secara keseluruhan. Meskipun frekuensi kejadiannya tidak selalu tinggi, konsekuensi yang ditimbulkan bersifat kritis karena seluruh layanan akademik berbasis sistem tidak dapat diakses.

Secara khusus, risiko R09 (server down) juga ditemukan sebagai risiko dominan dalam penelitian Rahayu et al. (2024), yang menunjukkan bahwa kestabilan server merupakan faktor kunci dalam menjaga keberlangsungan layanan sistem informasi. Dominasi risiko ini disebabkan oleh tingginya beban akses, terutama pada periode kritis seperti pengisian KRS, yang berpotensi menyebabkan overload pada server.

Implikasi dari risiko kategori tinggi ini tidak hanya berdampak pada aspek teknis, tetapi juga pada layanan akademik secara menyeluruh. Ketika terjadi listrik padam, gangguan ISP, atau server down, mahasiswa tidak dapat melakukan aktivitas penting seperti pengisian KRS, akses jadwal, maupun layanan administrasi akademik lainnya. Hal ini berpotensi menimbulkan keterlambatan proses akademik, penumpukan akses setelah sistem pulih, serta menurunnya kualitas layanan institusi. Oleh karena itu, ketiga risiko ini memerlukan prioritas utama dengan strategi perlakuan berupa mitigasi untuk meminimalkan kemungkinan dan dampaknya.

Risiko dengan kategori sedang mencakup R02 (petir), R03 (kebakaran), R04 (korsleting listrik), R06 (human error), R10 (backup failure), R12 (bug pada fitur KRS), R13 (overload), R15 (update gagal), dan R16 (error pada fitur tertentu). Risiko-risiko ini berada pada level sedang karena meskipun memiliki potensi mengganggu kinerja sistem, dampaknya cenderung bersifat parsial dan tidak selalu menghentikan seluruh layanan. Sebagai contoh, bug pada fitur KRS atau error pada fitur tertentu hanya memengaruhi sebagian fungsi sistem, namun tetap dapat menghambat proses akademik pada layanan tertentu. Selain itu, risiko seperti human error dan kegagalan update menunjukkan bahwa faktor internal pengelolaan sistem juga berkontribusi terhadap munculnya risiko. Jika tidak ditangani dengan baik, risiko kategori sedang ini berpotensi meningkat menjadi risiko tinggi, terutama pada periode dengan intensitas penggunaan yang tinggi.

Risiko dengan kategori rendah meliputi R07 (data dilihat oleh pihak tidak berwenang), R08 (pencurian hardware), R11 (ketidaksesuaian sistem dengan peraturan baru), dan R14 (kerusakan hardware). Risiko-risiko ini memiliki kemungkinan kejadian yang relatif kecil serta dampak yang tidak secara langsung mengganggu operasional utama sistem. Namun demikian, risiko seperti akses tidak sah terhadap data tetap memiliki implikasi terhadap aspek keamanan informasi dan kepercayaan

pengguna, sehingga tetap perlu diperhatikan dalam pengelolaan jangka panjang.

Meskipun telah dikategorikan ke dalam tingkat tinggi, sedang, dan rendah, seluruh risiko tetap diberikan rekomendasi perlakuan. Hal ini bertujuan agar setiap risiko memiliki strategi penanganan yang sesuai dengan tingkat prioritasnya, sehingga pengelolaan risiko dapat dilakukan secara komprehensif dan berkelanjutan dalam mendukung kualitas layanan akademik di Universitas XYZ.

4. Kesimpulan

Berdasarkan hasil penelitian mengenai analisis manajemen risiko menggunakan kerangka kerja ISO 31000:2018 pada website Academic Integrated System (AIS) Universitas XYZ, dapat disimpulkan bahwa terdapat 16 risiko yang berpotensi memengaruhi keberlangsungan dan kinerja sistem. Risiko tersebut diklasifikasikan ke dalam tiga tingkatan, yaitu tingkat tinggi, menengah, dan rendah. Risiko tingkat tinggi terdiri dari tiga risiko utama, yaitu listrik padam, gangguan Internet Service Provider (ISP), dan server down, yang memiliki dampak langsung terhadap terhentinya seluruh layanan sistem. Sementara itu, risiko tingkat menengah dan rendah cenderung memberikan dampak parsial, namun tetap berpotensi mengganggu kualitas layanan apabila tidak dikelola dengan baik.

Penelitian ini memberikan kontribusi aplikatif melalui pemetaan risiko, klasifikasi tingkat risiko, serta penyusunan rekomendasi perlakuan risiko yang disesuaikan dengan karakteristik operasional sistem AIS. Temuan menunjukkan bahwa risiko dominan tidak hanya dipengaruhi oleh faktor teknis, tetapi juga oleh faktor penggunaan sistem yang bersifat fluktuatif, terutama pada periode kritis seperti pengisian KRS, sehingga berdampak langsung terhadap layanan akademik di Universitas XYZ.

Rekomendasi perlakuan risiko disusun berdasarkan tingkat prioritas. Pada kategori risiko tinggi, langkah mitigasi yang diusulkan meliputi penyediaan Uninterruptible Power Supply (UPS) sebagai sumber listrik cadangan, penggunaan lebih dari satu penyedia layanan internet untuk menjaga kestabilan konektivitas, serta pemeriksaan dan pemeliharaan infrastruktur server secara berkala. Rekomendasi ini diharapkan dapat meningkatkan keandalan sistem dan meminimalkan potensi gangguan layanan akademik.

Adapun saran untuk penelitian selanjutnya adalah mengembangkan penelitian hingga tahap evaluasi dan monitoring risiko, sehingga efektivitas penerapan manajemen risiko dapat diukur secara berkelanjutan. Selain itu, penelitian selanjutnya juga dapat mempertimbangkan penggunaan atau perbandingan dengan kerangka kerja manajemen risiko lainnya untuk memperkaya analisis.

Daftar Pustaka :

Adhitya, A. G., & Suryadi, C. (2022). Pengembangan Model Pengelolaan Risiko Sistem Informasi Berbasis FMEA DAN ISO 31000:2009 Sebagai Pendukung K3L Di Laboratorium Lingkungan. *Jurnal Reka Lingkungan*, *10*(1), 79–90. https://doi.org/10.26760/rekalingkungan.v10i1.79-90

Ambarwati, R., Sulistiyowati, W., Kusno, Astutik, I. R. I., & Saputri, A. H. (2024). *Model Manajemen Teknologi Berbasis Risiko*. UMSIDA Press. https://press.umsida.ac.id/index.php/umsidapress/article/view/978-623-464-101-1

Fauziyah, S., & Sugiarti, Y. (2022). Literature Review: Analisis Metode Perancangan Sistem Informasi Akademik Berbasis Web. *Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer*, *8*(2), 87–93. https://doi.org/10.35329/jiik.v8i2.229

FKM UNMUL. (2023). *AIS (Academic Integrated System)*. Diakses pada 27 Februari 2025 https://fkm.unmul.ac.id/pages/akademikXais-academic-integrated-system-

Hardjomidjojo, H., Pranata, C., & Baigorria, G. (2022). Rapid assessment model on risk management based on ISO 31000:2018. *IOP Conference Series: Earth and Environmental Science*, *1063*(1). https://doi.org/10.1088/1755-1315/1063/1/012043

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. https://doi.org/10.35957/jatisi.v9i1.1478

Helmi, S., & Ariana, S. (2022). *Manajemen Perusahaan*. Jejak Pustaka. https://rie.binadarma.ac.id/file/book/manajemen-perusahaan-1670291653.pdf

Herlambang, A. A., Gani, A. A., & Alvianto, D. D. (2024). Pendekatan ISO 31000:2018 dalam Manajemen Risiko Teknologi Informasi pada Tracer Study Universitas Sebelas April. *Jurnal Intelek Dan Cendikiawan Nusantara*, *1*(4), 5651–5660. https://jicnusantara.com/index.php/jicn/article/download/924/1035

Huda, N., & Megawaty, M. (2021). Analisis Kinerja Website Dinas Komunikasi dan Informatika Menggunakan Metode Pieces. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *10*(2), 155–161. https://doi.org/10.32736/sisfokom.v10i2.1018

ISO. (2023). *Standar ISO 31000:2018*. 2023. Diakses pada 01 Maret 2025 https://www.iso.org/standard/65694.html

Izzudin, M. A., Informasi, S., Islam, U., Sunan, N., Surabaya, A., Wonosari, J., Sidoarjo, K., & Sidoarjo, D. K. (2024). *Analisis Risiko Menggunakan Iso 31000 : 2018 Dalam*

Pengelolaan Aplikasi Pada Kecamatan Dan OPD Kabupaten Sidoarjo. *8*(6), 12023–12029. https://ejournal.itn.ac.id/index.php/jati/article/view/11787/6632

Kevin Geofanny, G., & Rocky Tanaamah, A. (2022). Sistem Manajemen Risiko Berbasis ISO 31000:2018 Di PT. Bawen Mediatama. *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(4), 2870–2878. https://jurnal.mdp.ac.id/index.php/jatisi/article/view/2484

Muhammad Asir, Yuniawati, R. A., Mere, K., Sukardi, K., & Anwar, Muh. Abduh. (2023). Peran Manajemen Risiko Dalam Meningkatkan Kinerja Perusahaan: Studi Manajemen Sumber Daya Manusia. *Entrepreneurship Bisnis Manajemen Akuntansi (E-BISMA)*, *4*(1), 32–42. https://doi.org/10.37631/ebisma.v4i1.844

Mukhtar Syafii. (2022, July 4). *Perbedaan ISO 31000 Tahun 2009 dan 2018*. https://isoindonesiacenter.com/apa-itu-perbedaan-iso-31000-tahun-2009-dan-2018/

Oktavia, U. S. , Anugrah, I. G. , & Witra, W. P. P. (2025). *Analisis Manajemen Resiko Teknologi Informasi Pt. Eterindo Nusa Graha Menggunakan Framework ISO 31000:2018*. *16*(1), 100–119. https://ejurnal.provisi.ac.id/index.php/JTIKP/article/view/994

Prastiwi, A. P., Kholil, S., & Sumanti, S. T. (2022). Pengelolaan Website Dinas Komunikasi Dan Informatika Kabupaten Asahan Sebagai Akses Informasi Publik. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *1*(11), 2605–2614. https://doi.org/10.54443/sibatik.v1i11.399

Rachmadhani, M. (2022). *Desain Framework Manajemen Risiko Berbasis Iso 31000 Dan Scor Model* [Universitas Islam Indonesia]. https://dspace.uii.ac.id/handle/123456789/38882

Rahayu, S., Saputra, E., Luthfi Hamzah, M., Fronita, M., & Siregar, S. (2024). Analisis Manajemen Risiko Teknologi Informasi Pada Sistem TBS Dengan Metode ISO 31000 di PT XYZ. *Jurnal Pendidikan Dan Teknologi Indonesia*, *4*(12), 727–735. https://doi.org/10.52436/1.jpti.551

Salim, L. D., & Prasetyo, A. H. (2023). Rancangan Manajemen Risiko Dan Assesmen Risiko Pada Pt Pel Berlian Pulau Mandangin Berdasarkan Iso 31000:2018. *JURNALKU*, *3*(3), 242–268. https://pdfs.semanticscholar.org/6c28/823af952f1f7a86b87e7cf8e1cb14b9a8166.pdf

Setiawan, I., Sekarini, A. R., Waluyo, R., & Afiana, F. N. (2021). Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *20*(2), 389–396. https://doi.org/10.30812/matrik.v20i2.1093

Sitanggang, P. A., & Sitanggang, F. A. (2022). Analisis Implementasi Manajemen Risiko Berdasarkan SNI ISO 31000:2018 (Studi Kasus: Sparepart Personal Computer Second Jambi). *Eksis: Jurnal Ilmiah Ekonomi Dan Bisnis*, *13*(1), 12–19. https://doi.org/10.33087/eksis.v13i1.293

Tanamaah, A. R., & Berliana, L. D. (2021). Analisis Risiko Dengan Metode ISO 31000 Pada Disperinnaker Kota Salatiga Bidang Industri. *Jurnal Teknik Informatika Dan Sistem Informasi*, *8*(3), 1105–1118. https://jurnal.mdp.ac.id/index.php/jatisi/article/view/1037

Wattimena, A. M. G., & Tanaamah, A. R. (2021). Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 Pada TSI/Teknologi dan Sistem Informasi Perpustakaan UKSW. *Journal of Information Systems and Informatics*, *3*(3), 483–498. https://doi.org/10.51519/journalisi.v3i3.183

Wibowo, A. (2022). *Manajemen Risiko* (T. S. Santoso, Ed.). Yayasan Prima Agus Santoso. https://penerbit.stekom.ac.id/index.php/yayasanpat/article/download/341/373

Wirayudha, M. A., Novriyanto, N., Darmizal, T., & Oktavia, L. (2024). Analisis Manajemen Risiko Teknologi Informasi pada KPU Menggunakan Cobit 5 Domain APO12. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(2), 433–442. https://doi.org/10.57152/malcom.v4i2.1225

Yolanda, B., Nasrullah, M., & Kusumawati, A. (2024). Analisis Manajemen Risiko dengan Menggunakan Framework ISO 31000:2018 pada Sistem Informasi E-Gudang Satpol PP Kota Surabaya. *Jurnal Teknologi Informasi Dan Komunikasi*, *14*(2), 79–91. https://jurnal.unai.edu/index.php/teika/article/view/3483

Yuli Anita, S., Tanti Kustina, K., Wiratikusuma, Y., Sudirjo, F., Sari, D., Rupiwardani, I., Nugroho, L., Rakhmawati, I., Kesumawati Harahap, A., Anwar, S., Apriani, E., & Luh Ketut Ayu Sudha Sucandrawati, N. (2023). *Manajemen Risiko*. www.globaleksekutifteknologi.co.id

Yuwono, M. A., & Ellitan, L. (2023). *Enhancing Company Performance Through Risk Governance Evaluation Based on ERM ISO 31000:2018 Facilitated by Internal Auditors*. *1*(1), 2030–2040. https://journal.trunojoyo.ac.id/icembus