KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 6, No. 2, April (2025), pp. 468-477

Analisis Risiko Aplikasi HCMS PT. Bank SulutGo menggunakan ISO 31000

Regina Sophia Laode[1], Rudi Latuperissa[2]
[1,2]Universitas Kristen Satya Wacana, Indonesia
E-mail: 682021099@student.uksw.edu[1], rudi.latuperissa@uksw.edu[2]

Abstract

This study aims to analyze the risks contained in the Human Capital Management System (HCMS) application at PT Bank SulutGo using the ISO 31000 standard as a risk management framework. The research method used is qualitative, with data collection through literature studies, interviews with HCMS application admins, and direct observation of application business processes. The risk management process is carried out through the stages of communication and consultation, context setting, risk assessment (identification, analysis, and risk evaluation), and risk treatment according to ISO 31000 guidelines. The results showed that there were 11 main risks identified, which were grouped into human, environmental, and system factors. These risks include data input errors, password theft, lack of operator training, network disruptions, and data breaches. Risk analysis was conducted by assessing the probability and impact of each risk, then evaluated to determine the priority of handling. Proposed risk mitigation recommendations include increased training, strengthened system security, and improved data input procedures. In conclusion, a systematic approach to IT risk management is essential to maintain the sustainability and security of banking operations in the digital era.

Keywords: *Risk Management, ISO 31000, HCMS, Banking, Information Security.*

Abstrak

Penelitian ini bertujuan untuk menganalisis risiko yang terdapat pada aplikasi Human Capital Management System (HCMS) di PT. Bank SulutGo dengan menggunakan standar ISO 31000 sebagai kerangka manajemen risiko. Metode penelitian yang digunakan adalah kualitatif, dengan pengumpulan data melalui studi literatur, wawancara kepada para admin aplikasi HCMS, serta observasi langsung terhadap proses bisnis aplikasi. Proses manajemen risiko dilakukan melalui tahapan komunikasi dan konsultasi, penetapan konteks, penilaian risiko (identifikasi, analisis, dan evaluasi risiko), serta perlakuan risiko sesuai pedoman ISO 31000. Hasil penelitian menunjukkan terdapat 11 risiko utama yang teridentifikasi, yang dikelompokkan ke dalam faktor manusia, lingkungan, dan sistem. Risiko-risiko tersebut meliputi kesalahan input data, pencurian password, kurangnya pelatihan operator, gangguan jaringan, hingga pembobolan data. Analisis risiko dilakukan dengan menilai probabilitas dan dampak setiap risiko, kemudian dievaluasi untuk menentukan prioritas penanganan. Rekomendasi mitigasi risiko yang diusulkan antara lain peningkatan pelatihan, penguatan keamanan sistem, serta perbaikan prosedur input data. Kesimpulannya, pendekatan sistematis terhadap manajemen risiko TI sangat penting untuk menjaga keberlanjutan dan keamanan operasional perbankan di era digital.

Kata kunci: *Manajemen Risiko, ISO 31000, HCMS, Perbankan, Keamanan Informasi.*

1. Pendahuluan

Dalam era digital ini, Teknologi Informasi menjadi bagian penting bagi perusahaan perbankan termasuk PT. Bank Pembangunan Daerah Sulawesi Utara Gorontalo atau PT.

ISSN: 2720-992X

Bank SulutGo. Salah satu penggunaan Teknologi Informasi di PT. BSG adalah Aplikasi *Human Capital Management System* (HCMS). Dengan adanya HCMS, proses rekrutmen & seleksi, manajemen kinerja, penggajian, pelatihan, hingga pengembangan karyawan menjadi lebih efisien [1]. Namun dapat menimbulkan berbagai risiko seperti serangan siber, *human error*, dan kegagalan sistem [2]. Adapun risiko teknologi informasi ini erat kaitannya dengan keamanan informasi, di mana informasi merupakan sebuah aset yang sangat penting. Risiko yang muncul dapat menyebabkan proses bisnis berjalan tidak optimal dan berbagai hal yang dapat merugikan perusahaan [3].

Penelitian ini menggunakan metode ISO 31000 yang merupakan standar internasional yang menyediakan prinsip dan pedoman untuk manajemen risiko suatu perusahaan. Dalam perusahaan perbankan, manajemen risiko adalah elemen krusial untuk menjaga stabilitas dan keberlanjutan bisnis [2]. Manajemen Risiko adalah proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang dapat menghambat keberhasilan perusahaan [4]. Untuk meminimalisir risiko-risiko yang mungkin terjadi, penelitian ini menggunakan salah satu metode untuk manajemen risiko yaitu, ISO 31000. Metode ini dapat digunakan oleh perusahaan, asosiasi, kelompok, atau individu publik, swasta, atau komunitas mana pun. Standar ini fleksibel dan dapat diterapkan di berbagai aspek organisasi, mulai dari strategi dan pengambilan keputusan hingga operasional, proyek, proses, produk, fungsi, layanan, dan pengelolaan aset [5]. Manajemen Risiko terdiri dari 3 proses utama, yaitu Penetapan Konteks (*Esthablishing the Context*), Penilaian Risiko (*Risk Assessment*), dan Penanganan Risiko (*Risk Treatment*). Penilaian Risiko mencakup Indentifikasi Risiko, Analisis Risiko, dan Evaluasi Risiko. Selain itu, ada dua proses pendukung yang penting, yakni Komunikasi & Konsultasi, serta *Monitoring* & *Review* [6].

Dalam era digital saat ini, manajemen risiko teknologi informasi menjadi sangat penting bagi perusahaan untuk melindungi aset dan informasi yang berharga. Pentingnya manajemen risiko TI ini karena dapat membantu mengidentifikasi, menganalisis, mengendalikan, dan meminimalkan dampak risiko. Penelitian menggunakan ISO 31000:2018 oleh (*Krisdana Bima Mahardika et al., 2019*) untuk manajemen risiko pada CV.XY. Dari hasil penelitian tersebut, terdapat beberapa kemungkinan risiko dengan berbagai tingkatan dan rekomendasi yang diperlukan untuk meminimalisir berbagai risiko yang ada [7]. Hal ini sejalan dengan Penelitian manajemen risiko menggunakan ISO 31000:2018 juga dilakukan oleh *Jericho & Endang Haryani (2024)* pada Sistem Informasi Smart Operation dan ditemukan 12 risiko dengan berbagai tingkatan. Walaupun tidak ada risiko yang merugikan dan membahayakan perusahaan, peneliti merekomendasikan perlakuan risiko yang bisa mengurangi risiko [8].

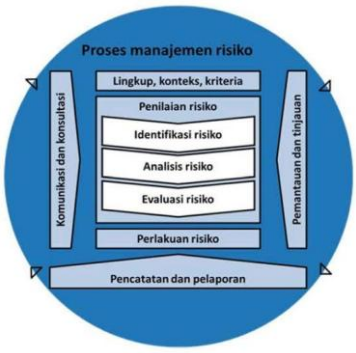
Penelitian oleh *Nola Novita & Evi Maria (2024)*, menggunakan standar ISO 31000:2018 untuk menganalisis manajemen risiko pada sistem informasi sekolah terpadu (SIKADU) SMKN 2 Salatiga. Dari penelitian yang dilakukan terdapat 22 kemungkinan risiko. Penelitian ini dilakukan agar dapat menjadi acuan bagi sekolah untuk dapat meminimalisir dan mengelola risiko, agar kinerja sistem dapat berjalan efektif dan efisien [9]. Berdasarkan penelitian pada UMKM Toko Zavier oleh *Rista Indrayati Dewi & Ilham (2023)* terdapat 6 risiko yang dapat memengaruhi kinerja toko. Untuk itu, penelitian ini menyarankan agar dilakukan perlakuan risiko untuk mengurangi terjadinya risiko dimasa yang akan datang [10]. Penelitian manajemen risiko menggunakan ISO 31000 juga dilakukan oleh (*Hanna Talitha et al., 2018*) untuk mengetahui risiko IT pada Sistem Penjualan Alphasos. Penelitian ini memberikan rekomendasi pengendalian yang tepat untuk setiap risiko yang peneliti dapati, namun tidak mencantumkan jumlah risiko pada kesimpulan [11].

Dengan demikian, manajemen risiko teknologi informasi bukan hanya berfokus pada upaya menghindari kerugian, tetapi juga bertujuan untuk menciptakan lingkungan yang aman, efisien, dan mendukung pencapaian tujuan strategis organisasi. Melalui penerapan pendekatan yang sistematis, berbasis data, dan sesuai standar ISO 31000, organisasi dapat

lebih siap menghadapi berbagai ketidakpastian sekaligus memanfaatkan peluang yang muncul di era digital yang terus berkembang.

2. Metodologi Penelitian

Penelitian kualitatif merupakan metode yang digunakan dalam penelitian ini. Metode penelitian ini berfokus pada pemahaman mendalam terhadap fenomena sosial melalui pengumpulan data deskriptif yang diperoleh dari wawancara, studi dokumen, dan observasi. Terdapat 3 tahapan penting dalam penelitian ini, pertama peneliti akan melakukan studi literatur terhadap penelitian-penelitian terdahulu. Kedua, akan dilakukan pengumpulan data dengan melakukan wawancara kepada Divisi *Human Capital* dan atau admin aplikasi HCMS. Ketiga adalah pengolahan data hasil wawancara dan analisa menggunakan ISO 31000.



Gambar 1. Proses Manajemen Risiko
Sumber: https://irmapa.org/wp-content/uploads/2019/11/2-1.jpg diakses 9 April 2025.

Tahap *Literature Review* akan dilakukan untuk mengumpulkan informasi sebagai landasan teori, serta mempelajari penelitian-penelitian sebelumnya yang memiliki studi kasus serupa. Informasi dari penelitian-penelitian tersebut akan digunakan sebagai referensi dalam penulisan jurnal ini. Teori-teori yang menjadi landasan penulisan berasal dari sejumlah sumber, termasuk jurnal ilmiah, skripsi, dan situs web resmi yang relevan dengan topik penelitian ini.

Metode pengumpulan data dalam peelitian ini akan dilakukan melalui wawancara langsung kepada pegawai Divisi Human Capital dan/atau admin Aplikasi HCMS, untuk memperoleh informasi yang mendalam terkait proses, tantangan, serta risiko yang dihadapi dalam pengelolaan aplikasi tersebut. Selain itu, observasi langsung juga akan dilakukan pada proses bisnis aplikasi HCMS untuk memastikan keakuratan data serta memahami alur kerja secara nyata. Kombinasi kedua metode ini diharapkan dapat memberikan gambaran yang komprehensif mengenai kondisi aktual serta potensi risiko yang ada pada implementasi dan operasional aplikasi HCMS.

Selanjutnya adalah Proses Manajemen Risiko berdasarkan ISO 31000:2018. Berdasarkan Gambar 1, berikut tahapan-tahapannya:

1. Komunikasi dan Konsultasi, pada tahap ini sangat diharapkan dapat tercipta dukungan yang memadai pada kegiatan manajemen risiko dan membuat kegiatan manajemen risiko menjadi tepat sasaran. Kolaborasi dan pemahaman bersama sangat penting untuk keberhasilan manajemen risiko. Komunikasi yang efektif dan konsultasi yang berkelanjutan memastikan semua pihak, yaitu peneliti dan perusahaan yang terlibat memiliki pandangan yang sama, berkontribusi secara optimal, dan proses pengumpulan data dapat berjalan lancar [6].
2. *Establishing the Context* atau Penetapan Konteks, menetapkan batasan yang jelas (ruang lingkup) dan memahami lingkungan operasional (konteks) adalah fondasi penting dalam manajemen risiko. Dalam penelitian ini, konteks yang akan diidentifikasi adalah analisis manajemen risiko TI pada aplikasi HCMS. Hal ini

dilakukan untuk memastikan penilaian risiko terfokus, relevan, dan menggunakan kriteria yang tepat, yaitu *likelihood* dan *impact* untuk mengukur tingkat risiko secara efektif [8].

3. Penilaian Risiko, tahap ini merupakan keseluruhan proses identifikasi risiko, analisis risiko, dan evaluasi risiko. Pada tahap ini akan ditetapkan kemunginan terjadinya dan dampak suatu peristiwa yang dapat menghalangi keberhasilan tujuan atau sasaran perusahaan dalam pengoperasian Aplikasi HCMS agar dapat dilakukan penanganan risiko secara tepat. Proses pertama adalah Identifikasi risiko (*Risk Identification*) yang dilakukan dengan menilai risiko. Menilai risiko dengan cara melihat potensi terjadinya seberapa besar probabilitas terjadinya risiko dengan membuat daftar kemungkinan kerugian yang mungkin terjadi dengan menggunakan teknik survey, wawancara interview, mengumpulkan informasi/data yang berkaitan dengan Aplikasi HCMS. Proses yang kedua adalah Analisis Risiko (*Risk Analysis*) yang merupakan suatu metode analisis yang meliputi faktor penilaian risiko yang harus dilakukan dengan tepat dan cermat agar mampu mengurangi kemungkinan terjadinya kerugian dari risiko yang terdapat pada Aplikasi HCMS. Analisis ini menggunakan tabel kriteria risiko *likelihood* dan *impact*. Kriteria *likelihood* digunakan untuk menentukan seberapa sering terjadinya risiko dan kriteria *impact* digunakan untuk menentukan seberapa besar dampak kerugian risiko terhadap perusahaan. Proses yang terakhir adalah Evaluasi Risiko (*Risk Evaluation*) yang akan membantu proses perlakuan keputusan risiko berdasarkan hasil dari analisis risiko yang akan menentukan risiko mana saja yang membutuhkan perlakuan khusus dan bagaimana prioritas perlakuannya. Evaluasi Risiko ini akan dibuat dengan menggunakan matriks risiko yang terdiri dari 3 level, yaitu *low*, *medium*, dan *high* [12].
4. Perlakuan Risiko, pada tahap ini akan diberikan rekomendasi berdasarkan hasil evaluasi risiko untuk mengurangi kemungkinan terjadinya suatu risiko ataupun mengurangi dampak kerusakan yang dihasilkan oleh risiko internal ataupun eksternal pada Aplikasi HCMS.

Tahap terakhir dalam penelitian ini adalah kesimpulan. Kesimpulan dari proses manajemen risiko adalah bahwa dengan melakukan identifikasi, analisis, evaluasi, dan penanganan risiko secara sistematis, perusahaan dapat mengelola risiko dengan lebih baik. Proses ini membantu perusahaan untuk meningkatkan kinerja, melindungi aset, dan mencapai tujuan dengan lebih efektif.

3. Hasil dan Pembahasan

Pada tahap ini, akan dilakukan penilaian terhadap kemungkinan terjadinya serta dampak dari suatu kejadian yang berpotensi menghambat pencapaian tujuan atau sasaran perusahaan dalam penggunaan Aplikasi HCMS dengan menggunakan pedoman ISO 31000, sehingga dapat diambil langkah-langkah pengelolaan risiko yang tepat.

3.1. Penilaian Risiko (*Risk Assessment*)

Pada tahap penilaian risiko, terdapat tiga proses utama yang harus dilakukan sesuai dengan pedoman ISO 31000, yaitu proses identifikasi risiko, analisis risiko, dan evaluasi risiko. Identifikasi risiko bertujuan untuk mengenali berbagai potensi risiko yang dapat mempengaruhi pencapaian tujuan organisasi. Setelah risiko diidentifikasi, langkah berikutnya adalah analisis risiko untuk menilai kemungkinan terjadinya dan dampak dari setiap risiko tersebut. Selanjutnya, dilakukan evaluasi risiko untuk menentukan prioritas penanganan berdasarkan tingkat risiko yang telah dianalisis, sehingga dapat diambil perlakuan risiko yang tepat dan efektif.

3.1.1. Identifikasi risiko (*Risk Identification*)

Identifikasi risiko merupakan proses awal dalam tahap penilaian risiko, dengan mengidentifikasi asset aplikasi HCMS, identifikasi risiko, dan identifikasi dampak. Pada proses ini akan dilakukan identifikasi terhadap asset-asset aplikasi HCMS berdasarkan komponen sistem informasi yaitu, data, *hardware*, dan *software*. Hal ini dilakukan agar seluruh potensi risiko yang mungkin terjadi diidentifikasi secara komprehensif dan didokumentasikan untuk dianalisis lebih mendalam.

Tabel 1. Identifikasi Asset Aplikasi HCMS

Komponen Sistem Informasi	Asset HCMS
Data	a. Data Pegawai b. Data Absensi & Kehadiran c. Data Penggajian d. Data Kinerja & Pengembangan e. Dokumen Kepatuhan & Legal
Hardware	a. Server *b. Computer* *c. Smartphone* *d. Scanner*
Software	Aplikasi HCMS (*Human Capital Management System*)

Berdasarkan proses identifikasi asset yang sudah dilakukan pada Tabel 1, terdapat 5 asset pada komponen data, 4 asset pada komponen *hardware*, dan 1 asset pada komponen *software*. Tahap berikutnya adalah melakukan identifikasi risiko yang dikelompokkan kedalam 3 faktor, yaitu faktor manusia, faktor lingkungan, dan faktor sistem. Tahap ini dilakukan untuk mengenali segala potensi ancaman yang dapat mempengaruhi keberlangsungan dan keamanan operasional aplikasi HCMS.

Tabel 2. Identifikasi Risiko

ID	Risiko	Faktor
R01	Kesalahan Input Nama, Marga, Data Diri Pegawai	Manusia
R02	Kesalahan Input *Grade*, Unit Kerja, Skala Gaji	
R03	Mutasi Pegawai	
R04	Kesalahan *Programming/Developer*	
R05	Pencurian *Password*	
R06	Kurangnya Pelatihan bagi Operator/Admin	
R07	Kesalahan Penginputan Data Diawal Masa Karir	
R08	Tidak Mengubah Kesalahan Input Data Pegawai Sampai pensiun	
R09	Jaringan Tidak Stabil	Lingkungan
R10	Server	
R11	Pembobolan Data	Sistem

Setelah dilakukan proses identifikasi risiko secara menyeluruh dan sistematis, ditemukan sebanyak 11 risiko yang diklasifikasikan ke dalam tiga kategori seperti pada Tabel 2. Proses selanjutnya adalah melakukan identifikasi dampak untuk menilai besarnya pengaruh risiko terhadap kegiatan operasional dan reputasi bank, sehingga dapat menentukan prioritas dalam pengelolaan risiko secara efektif.

Tabel 3. Identifikasi Dampak

Id	Risiko	Dampak
R01	Kesalahan Input Nama, Marga, Data Diri Pegawai	Data pegawai menjadi tidak akurat, berpotensi menimbulkan kesalahan administrasi, dan

Id	Risiko	Dampak
		mempengaruhi pengambilan keputusan.
R02	Kesalahan Input *Grade*, Unit Kerja, Skala Gaji	Terjadi kesalahan dalam perhitungan gaji, menimbulkan ketidakpuasan pegawai, serta potensi sengketa kompensasi.
R03	Mutasi Pegawai	Penempatan pegawai yang tidak sesuai dapat menurunkan motivasi kerja dan mengganggu produktivitas organisasi.
R04	Kesalahan *Programming/Developer*	Terjadinya bug atau *error* pada sistem yang berdampak pada kelancaran proses kerja..
R05	Pencurian *Password*	Akses tidak sah ke sistem yang dapat mengakibatkan pencurian data dan kerugian perusahaan.
R06	Kurangnya Pelatihan bagi Operator/Admin	Penurunan kompetensi, meningkatnya risiko kesalahan operasional, serta menurunnya efektivitas dan kualitas layanan organisasi.
R07	Kesalahan Penginputan Data Diawal Masa Karir	Data awal yang tidak tepat dapat menyebabkan kesulitan dalam pengelolaan pegawai dan kesalahan berkelanjutan.
R08	Tidak Mengubah Kesalahan Input Data Pegawai Sampai pensiun	Akumulasi kesalahan data yang tidak diperbaiki dapat menurunkan akurasi laporan.
R09	Jaringan Tidak Stabil	Data absensi menjadi tidak valid, berpotensi menimbulkan kesalahan dalam pengelolaan absensi dan penggajian.
R10	Server	Kebocoran data sensitif yang dapat merugikan perusahaan secara finansial dan reputasi.
R11	Pembobolan Data	Gangguan layanan akibat downtime server, yang dapat menyebabkan hilangnya data dan terganggunya operasional.

Proses identifikasi aset, risiko, dan dampak telah dilakukan secara menyeluruh dan sistematis. Sebanyak 11 risiko telah diidentifikasi, yang masing-masing memiliki potensi dampak signifikan terhadap operasional. Hasil identifikasi ini akan menjadi fondasi penting dalam mengembangkan strategi mitigasi dan pengelolaan risiko yang efektif, sehingga memastikan kelancaran operasional sistem dan mengurangi potensi kerugian.

3.1.2. Analisis Risiko (*Risk Analysis*)

Proses yang kedua adalah analisis risiko (*risk analysis*). Pada proses ini, dilakukan analisis terhadap risiko-risiko yang telah diidentifikasi dengan mempertimbangkan besarnya kemungkinan terjadinya (*Likelihood*) serta dampak yang ditimbulkan (*Impact*). Penilaian ini penting untuk menentukan tingkat risiko secara jelas dengan mengacu pada Tabel 4 yang mengukur seberapa besar kemungkinan risiko terjadi (*Likelihood*) berdasarkan kriteria *likelihood*, mulai dari *rare* sampai *certain* serta frekuensi kejadian risiko. Begitu juga dengan kriteria *impact* pada Tabel 5 yang juga digunakan untuk menilai tingkat keparahan risiko-risiko yang berdampak terhadap aspek penting bank mulai dari dampak paling kecil (*Insignificant*) sampai dengan dampak yang paling besar (*Catastrophic*).

Tabel 4. Kriteria *Likelihood*

Nilai	Kriteria	Deskripsi	Frekuensi
1	*Rare*	Risiko hampir tidak pernah terjadi	> 2 Tahun
2	*Unlikely*	Risiko Jarang Terjadi	1-2 Tahun
3	*Possible*	Risiko Kadang Terjadi	7-12 Bulan
4	*Likely*	Risiko Sering Terjadi	4-6 Bulan
5	*Certain*	Risiko hampir pasti terjadi	1-3 Bulan

Tabel 5. Kriteria *Impact*

Nilai	Kriteria	Deskripsi Dampak
1	*Insignificant*	Dampak sangat kecil, tidak mengganggu jalannya akivitas, kerugian minimal atau tidak signfikan.
2	*Minor*	Dampak ringan, sedikit mengganggu aktivitas, kerugian kecil
3	*Moderate*	Dampak sedang, mengganggu proses bisnis, menyebabkan keterlambatan atau gangguan sebagian aktivitas
4	*Major*	Dampak besar, hampir menghambat seluruh aktivitas, kerugian signifikan yang perlu diperhatikan serius
5	*Catastrophic*	Dampak sangat besar, menyebabkan proses bisnis berhenti total, kerugian besar dan berisiko tinggi

Proses selanjutnya akan dilakukan penilaian terhadap risiko-risiko yang ada berdasarkan kriteria *likelihood* dan *impact* pada Tabel 4 dan Tabel 5.

Tabel 6. Penilaian Risiko

ID	Risiko	*Likelihood*	*Impact*
R01	Kesalahan Input Nama, Marga, Data Diri Pegawai	2	2
R02	Kesalahan Input *Grade*, Unit Kerja, Skala Gaji	3	3
R03	Mutasi Pegawai	2	3
R04	Kesalahan *Programming/Developer*	2	3
R05	Pencurian *Password*	1	5
R06	Kurangnya Pelatihan bagi Operator/Admin	1	4
R07	Kesalahan Penginputan Data Diawal Masa Karir	1	2
R08	Tidak Mengubah Kesalahan Input Data Pegawai Sampai pensiun	1	4
R09	Jaringan Tidak Stabil	4	3
R10	Server	1	5
R11	Pembobolan Data	1	5

Penilaian risiko ini akan digunakan sebagai dasar untuk evaluasi risiko dan hasilnya akan dimasukkan ke dalam matriks risiko guna memetakan tingkat risiko secara jelas dan memudahkan pengambilan keputusan dalam pengelolaan risiko.

3.1.3. Evaluasi Risiko (*Risk Evaluation*)

Pada proses terakhir, yaitu evaluasi risiko, dilakukan pemetaan risiko menggunakan tabel matriks risiko yang membagi risiko ke dalam tiga *level of risk*, yaitu rendah (*low*), sedang (*medium*), dan tinggi (*high*), untuk memudahkan prioritas penanganan risiko secara efektif.

Tabel 7. Matriks Risiko

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

Tabel 8. Pemetaan Risiko

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

Berdasarkan hasil pemetaan risiko menggunakan kriteria *likelihood* dan *impact* pada Tabel 8, terdapat 2 risiko pada *level of risk* rendah (*low*) dan 9 risiko pada *level of risk* sedang (*medium*), sedangkan pada *level of risk* tinggi (*high*) tidak ditemukan risiko sama sekali. Selanjutnya, risiko-risiko yang telah diidentifikasi akan digabungkan dengan kriteria *likelihood* dan *impact* serta *level of risk* mulai dari level *medium* sampai *low* seperti yang ditampilkan/disajikan pada Tabel 9.

Tabel 9. Level Risiko

ID	Risiko	*Likelihood*	*Impact*	*Level Of Risk*
R02	Kesalahan Input *Grade*, Unit Kerja, Skala Gaji	3	3	Medium
R03	Mutasi Pegawai	2	3	Medium
R04	Kesalahan *Programming/Developer*	2	3	Medium
R05	Pencurian *Password*	1	5	Medium
R06	Kurangnya Pelatihan bagi Operator/Admin	1	4	Medium
R08	Tidak Mengubah Kesalahan Input Data Pegawai Sampai pensiun	1	4	Medium
R09	Jaringan Tidak Stabil	4	3	Medium
R10	Server	1	5	Medium
R11	Pembobolan Data	1	5	Medium
R01	Kesalahan Input Nama, Marga, Data Diri Pegawai	2	2	Low
R07	Kesalahan Penginputan Data Diawal Masa Karir	1	2	Low

Setelah dianalisis berdasarkan *level of risk*, terdapat 9 risiko yang termasuk dalam tingkat sedang (*medium*) dan 2 risiko yang berada pada tingkat rendah (*low*). Dengan demikian, fokus utama mitigasi perlu diarahkan pada risiko tingkat medium karena potensi dampaknya yang lebih signifikan, sementara risiko tingkat rendah tetap harus dipantau agar tidak berkembang menjadi masalah yang lebih besar di kemudian hari. Pendekatan ini membantu organisasi dalam mengelola risiko secara efektif dan menjaga keberlanjutan operasional serta pencapaian tujuan secara keseluruhan.

3.2. Perlakuan Risiko

Pada tahap ini akan dilakukan perlakuan risiko yang terdiri dari lima jenis, yaitu *Risk Avoidance, Risk Acceptance, Risk Sharing, Risk Exploit,* dan *Risk Mitigation.* Berdasarkan hasil identifikasi yang telah dilakukan, jenis perlakuan risiko yang paling tepat untuk aplikasi HCMS adalah mitigasi risiko (*Risk Mitigation*). Mitigasi risiko merupakan metode yang bertujuan untuk mengurangi kemungkinan terjadinya risiko maupun mengurangi dampak kerusakan yang ditimbulkan oleh risiko tersebut, sehingga dapat menjaga kelancaran operasional dan keamanan aplikasi secara efektif.

Tabel 10. Mitigasi Risiko

Level Of Risk	ID	Risiko	Mitigasi
Medium	R02	Kesalahan Input *Grade*, Unit Kerja, Skala Gaji	Menerapkan sistem validasi dan pengecekan ganda untuk meminimalkan kesalahan input.
Medium	R03	Mutasi Pegawai	Menggunakan sistem informasi terintegrasi untuk pencatatan mutasi secara akurat dan transparan
Medium	R04	Kesalahan *Programming/Developer*	Memberikan pelatihan dan standar pengembangan yang baik bagi *developer*.
Medium	R05	Pencurian *Password*	Terapkan *password* kompleks, autentikasi dua faktor, monitoring akses, dan pelatihan keamanan.
Medium	R06	Kurangnya Pelatihan bagi Operator/Admin	Menyediakan program pelatihan rutin dan komprehensif bagi operator dan admin serta melakukan evaluasi efektivitas pelatihan dan

Level Of Risk	ID	Risiko	Mitigasi
			pembaruan sesuai kebutuhan.
Medium	R08	Tidak Mengubah Kesalahan Input Data Pegawai Sampai pensiun	Menggunakan sistem *reminder* untuk memastikan koreksi data dilakukan tepat waktu dan menerapkan audit data berkala dan kebijakan perbaikan data.
Medium	R09	Jaringan Tidak Stabil	Melakukan pemeliharaan dan upgrade infrastruktur jaringan secara rutin.
Medium	R10	Server	*Backup* data secara rutin, menggunakan server dengan keamanan memadai, serta pemeliharaan dan *update* berkala.
Medium	R11	Pembobolan Data	Divisi IT akan melakukan *penetration test* atau simulasi *cyberattack* yang dilakukan oleh profesional terhadap aplikasi HCMS.
Low	R01	Kesalahan Input Nama, Marga, Data Diri Pegawai	Menerapkan validasi dan verifikasi data ganda saat menginput data.
Low	R07	Kesalahan Penginputan Data Diawal Masa Karir	Menggunakan *checklist* dan sistem verifikasi data awal.

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan pada aplikasi HCMS, ditemukan sebanyak 11 risiko yang berpotensi mempengaruhi kinerja dan keamanan sistem. Dari jumlah tersebut, 9 risiko termasuk dalam tingkat *medium*, yaitu risiko kesalahan input *grade*, unit kerja, skala gaji, mutasi pegawai, kesalahan *programming/developer*, pencurian *password*, kurangnya pelatihan bagi operator/admin, tidak mengubah kesalahan input data pegawai sampai pensiun, jaringan tidak stabil, server, dan risiko pembobolan data, yang memiliki tingkat keparahan dan kemungkinan terjadinya yang cukup tinggi sehingga memerlukan perhatian dan penanganan khusus agar dampak negatifnya dapat diminimalkan. Sedangkan pada tingkat *low* terdapat 2 risiko, yaitu risiko kesalahan input nama, marga, data diri pegawai dan kesalahan penginputan data diawal masa karir, yang meskipun memiliki potensi dampak yang lebih rendah, tetap harus dipantau dan dikelola dengan baik agar tidak berkembang menjadi masalah yang lebih serius di masa mendatang. Untuk setiap risiko yang telah diidentifikasi tersebut, diberikan mitigasi risiko yang dirancang secara khusus dan sistematis guna mengurangi kemungkinan terjadinya risiko serta mengendalikan dampak negatif yang mungkin timbul, sehingga keseluruhan pengelolaan risiko pada aplikasi HCMS dapat berjalan efektif dan mendukung tercapainya tujuan operasional dengan aman dan optimal.

Daftar Pustaka

[1] Admin, “Mengenal Apa itu Human Resource Management System,” 28 Juni. [Online]. Available: https://fitacademy.id/blog/mengenal-apa-itu-human-resource-management-system.

[2] Prospero, “Manajemen Risiko Operasional: Tantangan dan Solusi untuk Bank di Indonesia,” 3 Januari.

[3] “Langkah Menghindari Risiko dengan IT Risk Management,” 6 November. [Online]. Available: https://sisi.id/stories/insight/langkah-menghindari-risiko-dengan-it-risk-management/.

[4] P. SoM, “Manajemen Risiko: Pengertian, Manfaat dan Langkahnya,” 20 Juni. [Online]. Available: https://ppmschool.ac.id/manajemen-risiko/#Pengertian.

[5] ISO, “Manajemen Risiko — Prinsip dan Pedoman,” November. [Online]. Available: https://www-iso-org.translate.goog/standard/43170.html?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=sge.

[6] C. Kusuma, “Membedah Anatomi ISO 31000: 2009 Risk Management –

Principles and Guidelines." [Online]. Available: https://crmsindonesia.org/publications/membedah-anatomi-iso-31000-2009-risk-management-principles-and-guidelines/.

[7] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000 : 2018 (Studi Kasus: Cv. Xy)," *Sebatik*, vol. 23, no. 1, pp. 277–284, 2019, doi: 10.46984/sebatik.v23i1.572.

[8] E. Haryani, S. S. Informasi, F. T. Informasi, U. Kristen, and S. Wacana, "Penerapan ISO 31000 : 2018 untuk Analisis Manajemen Risiko pada Sistem Informasi Smart Operation di PT . XYZ," vol. 9, pp. 947–957, 2024.

[9] N. Novita Setyaningrum and E. Maria, "Penerapan Iso 31000:2018 Untuk Manajemen Risiko Pada Sistem Informasi Sekolah Terpadu," *J. Pendidik. Teknol. Inf.*, vol. 7, no. 1, pp. 31–44, 2024, doi: 10.37792/jukanti.v7i1.1164.

[10] R. I. Dewi and I. Ilham, "Analisis Manajemen Risiko pada UMKM Menggunakan Iso 31000," *J. Bisnis, Manajemen, Dan Inform.*, vol. 20, no. 2, pp. 124–135, 2023, doi: 10.26487/jbmi.v20i2.32130.

[11] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[12] Q. Dr Ir Dwi Rachmina, M.Si, "Penilaian Risiko – In General." [Online]. Available: https://irmapa.org/penilaian-risiko-in-general/.