JuSIN
Jurnal Sistem Informasi

Website: ojs.itb-ad.ac.id/index.php/JUSIN
E-ISSN: 2797-8516

ANALISIS MANAJEMEN RISIKO SISTEM INFORMASI AKUNTANSI PADA PT. BATU BARA XYZ ISO 31000:2018

Afifah Azzahra[1(*)], Putra Aditya[2], Sri Andayani[3]

[1]*Universitas Katolik Musi Charitas, Palembang*
[2]*Universitas Katolik Musi Charitas, Palembang*
[3]*Universitas Katolik Musi Charitas, Palembang*

Abstract

This study employs the ISO 31000:2018 framework to manage the accounting information system risks at PT. Batu Bara XYZ. It identifies, analyzes, evaluates, and treats risks accordingly. The findings reveal that classifying risks based on their likelihood and impact assists the company in planning effective risk management strategies. The implementation of the ISO 31000:2018 framework enables the company to better manage risks and enhance information security. The research aims to analyze the risk management of the accounting information system at PT. Batu Bara XYZ using the ISO 31000:2018 framework. A case study and quantitative approach were utilized as research methods. The study results demonstrate the identification, analysis, and evaluation of various potential risks affecting the company's accounting information system. This research is expected to provide insights into best practices and challenges faced, as well as offer recommendations for future risk management improvements.

Kata Kunci: Manajemen Resiko, ISO 3100:2018, Akuntansi, Sistem Informasi, Analisis

Januari – Juni 2024, Vol 5 (1) : hlm 41-50

(*) Korespondensi: affhazhhr3@gmail.com *(Afifah Azzahra)*

PENDAHULUAN

Dalam era revolusi industri 4.0, peranan teknologi informasi (TI) dalam mendukung efisiensi dan efektivitas operasional perusahaan menjadi sangat krusial. Hal ini berlaku universal di berbagai sektor, termasuk di industri pertambangan, di mana pengelolaan data dan informasi keuangan memegang peranan penting dalam pengambilan keputusan strategis. Namun, penggunaan TI yang intensif juga membawa risiko terhadap keamanan dan integritas data, yang menuntut implementasi manajemen risiko yang efektif (Utamajaya, Afrina and Fitriah, 2021).

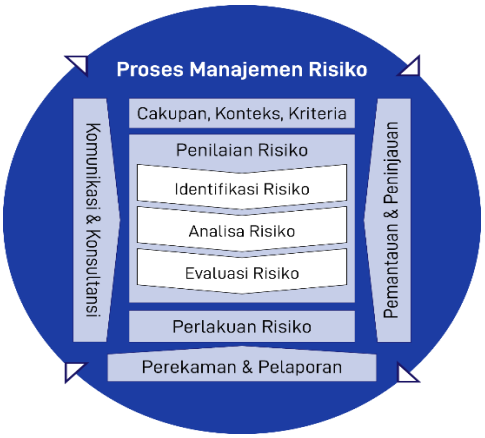
Penelitian terdahulu telah menunjukkan bahwa penerapan ISO 31000:2018 dapat membantu organisasi dalam mengidentifikasi, menganalisis, dan mengelola risiko TI, seperti yang terlihat pada studi kasus PT Pegadaian yang berhasil mengintegrasikan inovasi TI dalam layanan keuangannya (Linda Lole and Maria, 2022). Di sisi lain, penelitian pada PT Bawen Mediatama menyoroti pentingnya manajemen risiko dalam mengurangi insiden kecelakaan kerja, menunjukkan aplikasi ISO 31000:2018 dalam konteks keselamatan dan kesehatan kerja (Geofanny and Tanaamah, 2022).

Mengingat pentingnya manajemen risiko dalam pengelolaan Sistem Informasi Akuntansi, penelitian ini bertujuan untuk menganalisis bagaimana PT. Batu Bara XYZ menerapkan prinsip-prinsip ISO 31000:2018 dalam mengelola risiko yang terkait dengan Sistem Informasi Akuntansi. Analisis ini diharapkan dapat memberikan wawasan tentang praktik terbaik dan tantangan yang dihadapi, sekaligus memberikan rekomendasi untuk peningkatan manajemen risiko di masa depan (Wijaya, 2022).

METODE

Penelitian ini memanfaatkan pendekatan studi kasus yang bertujuan untuk meneliti secara mendalam penerapan sistem informasi akuntansi di PT. Batu Bara XYZ. Selain itu, peneliti juga mengadopsi metode kuantitatif dengan melakukan pengamatan langsung di lapangan untuk mengumpulkan data yang akurat.

Dalam penelitian ini, metode penelitian yang digunakan mengadopsi framework ISO 31000:2018. Prinsip-prinsip dan pedoman dari ISO 31000 dianggap sangat cocok untuk diterapkan dalam beragam konteks dan telah diakui secara global sebagai standar yang relevan dan efektif dalam manajemen risiko (Harefa, 2022).



Gambar 1. Proses Manajemen Risiko

Proses manajemen risiko meliputi 2 kegiatan yaitu risk assessment (penilaian risiko) dan risk treatment (perlakuan risiko). Penilaian risiko bertujuan untuk menentukan apakah risiko yang ada dalam sistem informasi akuntansi dapat diterima atau tidak. Ada beberapa langkah yang harus dilalui dalam proses menilai risiko tersebut, yaitu:

a. Identifikasi Risiko
   Langkah awal dalam proses manajemen risiko yang bertujuan untuk mengidentifikasi, menemukan, dan menjelaskan semua jenis risiko yang mungkin memengaruhi pencapaian tujuan atau sasaran suatu perusahaan.
b. Analisis Risiko
   Untuk memperoleh pemahaman yang lebih mendalam tentang risiko, hasil analisis risiko ini akan menjadi input bagi evaluasi risiko dan proses pengambilan keputusan mengenai cara menghadapi risiko tersebut.
c. Evaluasi Risiko
   Tahap terakhir melibatkan perbandingan hasil analisis dari setiap risiko terhadap kriteria risiko yang telah ditetapkan, dengan tujuan menentukan apakah langkah-langkah tambahan perlu diambil terhadap risiko tersebut.

HASIL DAN PEMBAHASAN

A. Penilaian Risiko (Risk Assessment)

1. Identifikasi Risiko

a. Identifikasi Aset

Pada tahap ini, dilakukan pengidentifikasian aset pada sistem informasi akuntansi, yang mencakup aset data, perangkat lunak, dan perangkat keras perusahaan.

Tabel 1. Identifikasi Aset pada sistem informasi akuntansi

Komponen SI/TI	Aset
Data	Data barang keluar
	Data barang masuk
	Data penjualan
	Data pembelian
	Data laporan laba rugi
	Data laporan arus kas
	Data laporan neraca
Software	Sistem informasi akuntasi PT. Batu Bara XYZ
Hardware	Komputer
	Mouse
	Keyboard
	CPU
	Printer
	Wifi

Tabel 1 diatas menunjukkan aset perusahaan yaitu data, software serta hardware yang mendukung adanya sistem informasi akuntansi.

b. Identifikasi Kemungkinan Risiko

Setelah mengidentifikasi aset dalam sistem informasi akuntansi di PT. Batu Bara XYZ, langkah berikutnya adalah mengidentifikasi risiko yang mungkin terjadi dengan mengelompokkannya berdasarkan berbagai faktor seperti lingkungan, sumber daya manusia (SDM), serta sistem dan infrastruktur.

Tabel 2. Identifikasi Kemungkinan Risiko

Faktor	Id	Kemungkinan Risiko
Alam atau Lingkungan	R01	Gempa Bumi
	R02	Banjir
	R03	Badai
	R04	Petir
	R05	Listrik Mati
	R06	Kebakaran
Manusia	R07	Human Error
	R08	Cybercrime
	R09	Penyalahgunaan hak akses
	R10	Pencurian data
Sistem dan Infrastruktur	R11	Maintenance yang tidak terjadwal
	R12	Server down
	R13	Koneksi jaringan tidak stabil
	R14	Koneksi jaringan tiba-tiba terputus
	R15	Serangan virus
	R16	Overhead
	R17	Sistem Crash

c. Identifkasi Dampak Risiko

Langkah berikutnya adalah melakukan identifikasi risiko dengan mengevaluasi dampak-dampak yang timbul dari kemungkinan risiko yang telah ditemukan dari identifikasi risiko sebelumnya.

Tabel 3. Identifikasi Dampak Risiko

Id	**Kemungkinan Risiko**	**Dampak**
R01	Gempa Bumi	Menyebabkan gangguan serius pada operasional sistem informasi akuntansi, bahkan mungkin menyebabkan kegagalan total.
R02	Banjir	Merusak peralatan fisik, kerusakan pada infrastruktur, serta kemungkinan kehilangan data yang disimpan di lokasi terendam air.
R03	Badai	Gangguan pada infrastruktur, kemungkinan pemadaman listrik, serta kerusakan pada bangunan dan peralatan.
R04	Petir	Kerusakan peralatan dan infrastruktur akibat lonjakan listrik yang dapat mengganggu operasional sistem informasi akuntansi.
R05	Listrik Mati	Gangguan langsung pada operasional sistem informasi akuntansi, yang

		mungkin mengakibatkan kehilangan data dan gangguan pada proses bisnis.
R06	Kebakaran	Kerusakan fisik pada bangunan, peralatan, dan infrastruktur yang dapat menyebabkan kegagalan sistem informasi akuntansi serta potensi kehilangan data yang signifikan.
R07	Human Error	Menyebabkan kerugian finansial, kehilangan data, dan reputasi perusahaan.
R08	Cybercrime	Pencurian data sensitif, kerusakan pada sistem, gangguan pada layanan, dan ancaman terhadap keamanan informasi yang dapat mengganggu kinerja sistem informasi akuntansi.
R09	Penyalahgunaan hak akses	Potensi pencurian atau manipulasi data, kebocoran informasi rahasia, dan gangguan pada operasional sistem akuntansi.
R10	Pencurian data	Kehilangan data sensitif, kerugian finansial, kerusakan reputasi, serta potensi pelanggaran privasi dan kepatuhan.
R11	Maintenance yang tidak terjadwal	Gangguan pada operasional sistem informasi akuntansi karena perawatan yang tidak terjadwal dapat mengganggu akses dan ketersediaan sistem.
R12	Server Down	Kegagalan pada server dapat mengakibatkan gangguan pada layanan, penurunan produktivitas, dan kehilangan data yang disimpan di server.
R13	Koneksi jaringan tidak stabil	Menyebabkan lambatnya kinerja sistem, kehilangan koneksi ke server, dan ketidakmampuan untuk mengakses data.
R14	Koneksi jaringan tiba-tiba terputus	Mengganggu operasional sistem informasi akuntansi dan menyebabkan kehilangan konektivitas.
R15	Serangan virus	Menyebabkan kerusakan pada sistem, kehilangan data, gangguan pada layanan, dan potensi pencurian informasi sensitif.
R16	Overhead	Menyebabkan penambahan waktu yang dibutuhkan untuk menyelesaikan tugas, yang menghasilkan penambahan latensi dalam respons sistem.
R17	Sistem Carsh	Menyebabkan gangguan pada operasional, kehilangan data, dan

	kerugian finansial akibat penurunan produktivitas dan pemulihan sistem.

2. Analisis Risiko

Pada tahap ini, risiko-risiko yang telah diidentifikasi sebelumnya dianalisis dengan menilai kemungkinan terjadinya. Proses ini melibatkan penggunaan tabel kriteria kemungkinan yang dibagi menjadi lima kriteria berdasarkan tingkat kejadian dalam periode waktu tertentu. Tabel 4 menunjukkan nilai likelihood.

Tabel 4. Nilai Likelihood

Nilai	Likelihood	Deskripsi
1.	*Rare*	Hampir tidak pernah terjadi atau mungkin terjadinya kecil >5 tahun
2.	*Unlikely*	Kemungkinan kecil terjadi 3-5 tahun
3.	*Possible*	Kemungkinan terkadang terjadi 2-4 tahun
4.	*Likely*	Kemungkinan besar terjadi 1-2 tahun
5.	*Almost Certain*	Hampir pasti terjadi < 1 tahun

Selanjunya adalah melakukan evaluasi terhadap dampak atau pengaruh yang mungkin terjadi pada objek kasus sebagai akibat dari kemungkinan risiko. Dalam penilaian dampak ini, dibedakan berdasarkan seberapa besar dampaknya terhadap kinerja sistem informasi akuntansi.

Tabel 5. Nilai Kriteria Impact

Nilai	Impact	Deskripsi
1.	*Insignificant*	Risiko yang tidak menghalangi aktivitas proses bisnis
2.	*Minor*	Risiko yang sedikit menghalangi aktivitas proses bisnis
3.	*Moderate*	Risiko yang cukup menghalangi aktivitas proses bisnis
4.	*High*	Risiko yang menghalangi aktivitas proses bisnis
5,	*Major*	Risiko yang sangat menghalangi aktivitas proses bisnis

Selanjutnya, akan dilakukan penilaian terhadap kemungkinan risiko berdasarkan nilai kemungkinan dan dampak yang terdapat dalam Tabel 4 dan Tabel 5.

Tabel 6. Penilaian Likelihood dan Impact

Id	Kemungkinan Risiko	Likelihood	Impact
R01	Gempa Bumi	1	4
R02	Banjir	2	4
R03	Badai	2	3
R04	Petir	2	2
R05	Listrik Mati	4	3
R06	Kebakaran	1	5
R07	Human Error	3	3
R08	Cybercrime	2	4
R09	Penyalahgunaan hak akses	3	2
R10	Pencurian data	1	4
R11	Maintenance yang tidak terjadwal	5	4
R12	Server Down	4	5
R13	Koneksi jaringan tidak stabil	3	5
R14	Koneksi jaringan tiba-tiba terputus	3	5

R15	Serangan virus	1	5
R16	Overhead	2	3
R17	Sistem Carsh	4	3

Dari Tabel 6 ditemukan nilai kemungkinan dan dampak terhadap risiko yang terdapat pada sistem informasi akuntansi PT. Batu Bara XYZ.

3. Evaluasi Risiko

Pada tahap evaluasi risiko, penilaian peringkat risiko memerlukan matriks yang memuat kombinasi antara tingkat kemungkinan dan dampak. Dengan menggunakan data dari tabel hasil analisis risiko, dilakukan representasi grafis dari peringkat risiko dengan mengalikan nilai kemungkinan dan nilai dampak pada sistem informasi akuntansi.

Tabel 7. Matrix Evaluasi Risiko

Likelihood							
	Certain	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Posisible	3	Low	Medium	Medium	Medium	High
	Unlikely	2	Low	Low	Medium	Medium	Medium
	Rare	1	Low	Low	Low	Medium	Medium
	Impact		1 Insigficant	2 Minor	3 Moderate	4 Major	5 Catastrophic

Risiko-risiko akan dikelompokkan berdasarkan tingkat risiko, dimulai dari yang paling tinggi hingga yang terendah, seperti yang dijelaskan dalam Tabel 7.

Setiap Id risiko akan kemudian ditempatkan dalam matriks evaluasi risiko sesuai dengan kriteria kemungkinan dan dampak.

Tabel 8. Matrik Evaluasi Risiko berdasarkan *Likelihood dan Impact*

Likelihood							
	Certain	5				R11	
	Likely	4			R17 R05		R12
	Posisible	3		R09	R07		R13 R14
	Unlikely	2		R04	R03 R16	R02 R08	
	Rare	1				R01 R10	R06 R15
	Impact		1 Insigficant	2 Minor	3 Moderate	4 Major	5 Catastrophic

Tabel 8 melakukan perhitungan kemungkinan dan dampak dari 17 kemungkinan risiko yang dapat dikelompokkan berdasarkan rasio. Kemudian, risiko-risiko tersebut akan dikelompokkan ke dalam tingkatan level high, medium, dan low sesuai dengan hasil perhitungan tersebut.

Tabel 9. Pengelompokkan Risiko Berdasarkan Tingkatan

Id	Kemungkinan Risiko	Likelihood	Impact	Risk Level
R13	Koneksi jaringan tiba-tiba tidak stabil	**3**	**5**	**High**
R14	Koneksi jaringan tiba-tiba terputus	**3**	**5**	**High**

R12	Server Down	**4**	**5**	**High**
R11	Maintenance yang tidak terjadwal	**5**	**4**	**High**
R17	Sistem Crash	**4**	**3**	**Medium**
R05	Listrik Mati	**4**	**3**	**Medium**
R07	Human Error	**3**	**3**	**Medium**
R03	Badai	**2**	**3**	**Medium**
R09	Penyalahgunaan hak akses	**3**	**2**	**Medium**
R10	Pencurian data	**1**	**4**	**Medium**
R01	Gempa Bumi	**1**	**4**	**Medium**
R02	Banjir	**2**	**4**	**Medium**
R08	Cybercrime	**2**	**4**	**Medium**
R06	Kebakaran	**1**	**5**	**Medium**
R15	Serangan Virus	**1**	**5**	**Medium**
R16	Overhead	**2**	**3**	**Medium**
R04	Petir	**2**	**2**	**Low**

Dari Tabel 9, terdapat hasil evaluasi risiko yang mencakup 17 kemungkinan yang diduga. Risiko-risiko tersebut telah dianalisis dan dikelompokkan berdasarkan tingkat risikonya. Sebanyak 4 risiko memiliki tingkat risiko tinggi, yaitu R11, E12, R13, dan R14. Selanjutnya, ada 12 risiko dengan tingkat risiko sedang, yaitu R17, R05, R07, R03, R09, R10, R11, R02, R08, R06, R15, dan R16. Hanya terdapat 1 risiko dengan tingkat risiko rendah, yaitu R04.

B. Perlakuan Risiko (Risk Treatment)

Setelah analisis risiko dilakukan, langkah berikutnya adalah tahap perlakuan isiko (risk treatment). Dalam tahap ini, dilakukan penyusunan rencana tindakan untuk mengatasi kemungkinan risiko yang telah dikelompokkan berdasarkan tingkat risiko.

Tabel 10. Usulan Perilaku Risiko

Id	Kemungkinan Risiko	Risk Level	Tindakan risiko
R13	Koneksi jaringan tiba-tiba tidak stabil	**High**	Memiliki cadangan koneksi internet dari penyedia layanan yang berbeda.
R14	Koneksi jaringan tiba-tiba terputus	**High**	Membuat dan mengimplementasikan rencana pemulihan bencana yang mencakup penggunaan koneksi backup dan solusi failover.
R12	Server Down	**High**	Memiliki tim teknis yang siap siaga untuk merespons dan memperbaiki masalah server dengan cepat.
R11	Maintenance yang tidak terjadwal	**High**	Menjadwalkan pemeliharaan secara berkala dan memberikan pemberitahuan kepada pengguna tentang jadwal pemeliharaan.
R17	Sistem Crash	**Medium**	Memiliki prosedur pemulihan sistem yang teruji dan diuji secara berkala.

R05	Listrik Mati	**Medium**	Menggunakan generator cadangan atau pasokan daya darurat untuk menjaga operasionalitas sistem selama pemadaman listrik.
R07	Human Error	**Medium**	Memberikan pelatihan kepada staf untuk meminimalkan kesalahan manusia.
R03	Badai	**Medium**	Memiliki rencana bencana yang mencakup tindakan untuk mengamankan infrastruktur fisik dari kerusakan yang disebabkan oleh badai.
R09	Penyalahgunaan hak akses	**Medium**	Menerapkan kontrol akses yang ketat dan melakukan pemantauan aktivitas pengguna secara teratur.
R10	Pencurian data	**Medium**	Mengenkripsi data sensitif dan mengimplementasikan tindakan keamanan yang kuat seperti otentikasi dua faktor.
R01	Gempa Bumi	**Medium**	Memiliki rencana evakuasi dan pemulihan pasca-gempa yang jelas.
R02	Banjir	**Medium**	Memastikan peralatan dan infrastruktur fisik ditempatkan dilokasi yang aman banjir.
R08	Cybercrime	**Medium**	Menggunakan solusi keamanan informasi seperti firewall, antivirus dan deteksi intrusi.
R06	Kebakaran	**Medium**	Memiliki sistem deteksi kebaran yang terpasang dengan baik.
R15	Serangan Virus	**Medium**	Menggunakan solusi antivirus yang kuat dan melakukan pemindaian secara berkala.
R16	Overhead	**Medium**	Memantau dan mengelola beban kerja sistem secara teratur untuk mencegah overhead yang tidak perlu.
R04	Petir	**Low**	Menggunakan sistem penangkal petir dan melindungi peralatan hardware dengan surge protector.

Pada tabel 10 diharapkan dapat meminimalisirkan kemungkinan risiko apa saja yang akan terjadi pada sistem informasi akuntansi.

KESIMPULAN

Berdasarkan penelitian terhadap Manajemen Risiko Sistem Informasi Akuntansi di PT. BatuBara XYZ dengan menggunakan framework ISO 31000:2018, dapat disimpulkan bahwa

identifikasi, analisis, dan evaluasi risiko secara sistematis sangat penting dalam mengelola risiko. Dengan mengklasifikasikan risiko berdasarkan tingkat likelihood dan impact ke dalam kategori tinggi, menengah, dan rendah, perusahaan dapat merencanakan dan mengimplementasikan strategi penanganan risiko secara efektif. Strategi tersebut meliputi memiliki cadangan koneksi internet, membuat rencana pemulihan bencana, menjadwalkan pemeliharaan secara berkala, dan menggunakan solusi keamanan informasi. Penerapan framework ISO 31000:2018 memungkinkan PT. BatuBara XYZ untuk mengelola risiko dengan lebih baik, memastikan kelangsungan operasional, dan meningkatkan keamanan informasi.

DAFTAR PUSTAKA

Geofanny, G.K. and Tanaamah, A.R. (2022) '***Sistem Manajemen Risiko Berbasis ISO 31000:2018 Di PT. Bawen Mediatama***', *JATISI (Jurnal Informatika dan Sistem Informasi)*, 9(4), pp. 2870–2878.

Harefa, W. (2022) '***Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang***', *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, 9(1), pp. 407–420. Available at: https://doi.org/10.35957/jatisi.v9i1.1478.

Linda Lole, K.M. and Maria, E. (2022) '***Analisis Manajemen Risiko Pada Aplikasi Pegadaian Digital Service Menu Tabungan Emas Menggunakan ISO 31000:2018***', *Jurnal Sistem Komputer dan Informatika (JSON)*, 3(3), p. 319. Available at: https://doi.org/10.30865/json.v3i3.3891.

Utamajaya, J.N., Afrina, A. and Fitriah, A.N. (2021) '***Analisis Manajemen Risiko Teknologi Informasi Pada Perusahaan Toko Ujung Pandang Grosir Penajam Paser Utara Menggunakan Framework Iso 31000:2018***', *Sebatik*, 25(2), pp. 326–334. Available at: https://doi.org/10.46984/sebatik.v25i2.1430.

Wijaya, V.P.P. (2022) '***Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018***', *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, 9(2), pp. 1295–1307. Available at: https://doi.org/10.35957/jatisi.v9i2.2087.