KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 4, No 2, Oktober 2023, Hal 1042-1051
DOI 10.30865/klik.v4i2.1174
https://djournals.com/klik

Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2018

Devara Liko Ivander, Frederik Samuel Papilaya*

Fakultas Teknologi Informasi, Sistem Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia
Email: 1,*682020033@student.uksw.edu, 2,*samuel.papilaya@uksw.edu
Email Penulis Korespondensi: samuel.papilaya@uksw.edu

Abstrak−Teknologi Informasi adalah inovasi berupa artefak, teknik, dan pengetahuan yang dapat memecahkan masalah manusia. Namun, penggunaannya harus dilakukan dengan pemahaman yang baik untuk menghindari berbagai macam risiko yang dapat merugikan banyak pihak. PT XYZ cabang Bawen merupakan perusahaan manufaktur kemasan karton box dan karton sheet yang telah berdiri sejak tahun 1995 dan terletak di Kecamatan Bawen, Kabupaten Semarang, Jawa Tengah. PT XYZ sudah menerapkan SI/TI dalam proses bisnisnya di mana SI/TI dapat membantu meningkatkan efisiensi proses dalam bisnis. Namun, perlu diketahui bahwa penerapan SI/TI tidak serta merta dapat berjalan dengan lancar dan tentu masih memiliki kekurangannya tersendiri. Oleh karena itu, penelitian ini bertujuan untuk mengetahui, menilai, dan meminimalisir risiko yang ada dalam PT XYZ dengan menggunakan framework ISO 31000:2018. Dari penelitian ini, ditemukan 26 kemungkinan risiko yang dapat terjadi di dalam perusahaan, dan dari 26 kemungkinan risiko, terdapat 15 risiko dengan tingkat risiko rendah (*low*), 5 risiko dengan tingkat risiko menengah (*medium*), 5 risiko dengan tingkat risiko menengah tinggi (*medium high*), dan 1 risiko dengan tingkat risiko tinggi (*high*). Dari risiko-risiko yang telah ditemukan, peneliti memberikan saran atau rekomendasi dalam menangani risiko, agar perusahaan mampu meminimalisir risiko yang ada dan dapat merasakan manfaat penelitian yang dilakukan, sesuai dengan tujuan penelitian ini. Perusahaan perlu dengan cermat menilai dan mengatasi risiko yang terkait dengan adopsi teknologi untuk memastikan kelancaran fungsi proses bisnis mereka dan melindungi diri dari hasil yang merugikan.

Kata Kunci: Analisis Risiko; Manajemen Risiko; ISO 31000:2018; Teknologi Informasi; Bawen

Abstract−Information Technology is an innovation encompassing artifacts, techniques, and knowledge that can solve human problems. However, its utilization must be accompanied by a thorough understanding to prevent various risks that could adversely affect multiple parties. PT XYZ Bawen Branch is a manufacturing company specializing in cardboard box and cardboard sheet packaging, established since 1995 and situated in the Bawen Subdistrict, Semarang Regency, Central Java. PT XYZ has incorporated IT/IS in its business processes, where IT/IS can enhance operational efficiency. Nonetheless, it's important to note that the implementation of IT/IS doesn't always proceed seamlessly and inherently carries its own shortcomings. Hence, this study aims to identify, assess, and mitigate the existing risks within PT XYZ using the ISO 31000:2018 framework. From this research, 26 potential risks were identified within the company. Out of these, there are 15 risks classified as low-risk, 5 as medium-risk, 5 as medium-high-risk, and 1 as high-risk. Among the discovered risks, the researchers offer suggestions or recommendations for risk management, enabling the company to minimize the identified risks and reap the benefits of this research, aligning with the research objectives. Companies need to carefully assess and address risks associated with technology adoption to ensure the smooth functioning of their business processes and to safeguard against any adverse outcomes.

Keywords: Risk Analysis; Risk Management; ISO 31000:2018; Information Technology; Bawen

1. PENDAHULUAN

Teknologi Informasi dianggap sebagai sebuah inovasi berupa artefak, teknik, serta pengetahuan yang mampu memecahkan permasalahan-permasalahan manusia yang meliputi pemanfaatan komputer bahkan hingga pemanfaatan satelit [1]. Dengan adanya Teknologi Informasi, manusia bisa saling bekerja sama tanpa dibatasi oleh jarak, waktu, dan faktor lain yang menghambat bentuk kerja sama antarmanusia [2]. Namun, pemanfaatan Sistem Informasi atau Teknologi Informasi (SI/TI) tentunya juga harus melibatkan pengguna yang memahami apa, bagaimana, kapan, mengapa, dan di mana serta dampak-dampak dari penggunaan Teknologi Informasi, karena tentunya penerapan Teknologi Informasi haruslah membantu dan bukan menghambat pencapaian tujuan organisasi, sehingga menghindari risiko kesalahan penggunaan dan penyalahgunaannya yang dapat menimbulkan berbagai macam masalah seperti penyalahgunaan data, pencurian, dan penjualan data individu hingga data-data krusial perusahaan, organisasi, ataupun suatu instansi [3], [4].

Di samping faktor kesiapan pengguna itu sendiri, masih banyak faktor-faktor lain yang juga kadang kala tidak diketahui oleh pengguna itu sendiri, di mana masa depan adalah hal yang tak pasti dan tak ada yang berhasil meramalkan kepastian di masa depan sehingga menyebabkan kesulitan dalam mengambil keputusan di bawah ketakutan akan ancaman-ancaman yang dapat muncul [5], [6], terkhususnya jika penggunaan teknologi informasi berada dalam skala besar layaknya di dalam perusahaan, organisasi, ataupun suatu instansi. Dalam pengimplementasian manajemen risiko, tentu terdapat faktor penentu keberhasilan yang sangat bergantung pada kondisi organisasi yang ada dan masih menjadi permasalahan atau topik pembahasan yang penting. Keberagaman kondisi risiko yang dihadapi tentu mempengaruhi ragam cara pengimplementasian manajemen risiko, sehingga setiap organisasi juga memiliki permasalahan risiko yang berbeda dan cara menghadapi yang sangat beragam pula [7]. Oleh karena itu, diperlukannya pengendalian atau kontrol dan strategi terhadap risiko-risiko yang mungkin dapat terjadi dengan mengidentifikasi, mengukur, dan memikirkan solusi terhadap ancaman-ancaman yang sekiranya dapat muncul di masa mendatang sebagai upaya antisipasi kecurangan dan penyalahgunaan teknologi yang ada [8].

Manajemen risiko dapat diterapkan dengan berpedoman pada ISO 31000:2018 yang bertujuan untuk pengarahan dan pengendalian terkait dengan risiko di dalam organisasi, serta membantu organisasi dalam mengembangkan strategi

manajemen risiko, agar risiko dapat diidentifikasi dan dimitigasi secara efektif, sehingga dapat meningkatkan kemungkinan pencapaian tujuan organisasi, dan peningkatan perlindungan terhadap aset-aset penting yang berkaitan dengan kelancaran proses bisnis organisasi itu sendiri [9], [10]. Aset-aset penting organisasi tidak hanya aset fisik saja, *stakeholder* atau pemangku kepentingan dalam tiap-tiap bagian organisasi juga sebagai aset yang mampu membawa risiko yang dapat saja disebabkan akibat *human error* [11]. Setiap organisasi harus mampu mengenali risiko-risiko yang ada, dengan harapan bahwa risiko yang ada dapat dicegah, dihindari, atau dikurangi dampaknya, untuk memperkuat dan membangun fondasi proses bisnis yang solid di masa mendatang dan terhindar dari risiko kehilangan peluang bisnis dan aset berharga.

PT XYZ cabang Bawen merupakan perusahaan manufaktur kemasan *karton box* dan *karton sheet* yang telah berdiri sejak tahun 1995 dan terletak di Kecamatan Bawen, Kabupaten Semarang, Jawa Tengah. PT XYZ sendiri telah mengimplementasikan SI/TI dalam memanajemen data-data penting perusahaan, seperti penggunaan aplikasi SAP untuk mengolah data-data dalam perusahaan serta pemanfaatan server lokal dan non-lokal. Namun, pemanfaatan SI/TI tidak serta merta berjalan lancar di dalam perusahaan. Sarana dan prasarana TI dalam PT XYZ masih tidak terhindar dari risiko-risiko seperti jaringan *down*/lambat/terputus, kurangnya implementasi keamanan fisik TI, hingga kerusakan *storage*. Hal tersebut tentu dapat mengganggu kelancaran dan keamanan proses bisnis yang ada dalam perusahaan akibat dari risiko-risiko yang ada saat ini, sehingga manajemen risiko sangatlah penting dilaksanakan demi mengurangi dan mencegah risiko-risiko yang sekiranya akan mengancam di masa depan [12], [13], [14].

Terdapat banyak penelitian terdahulu yang pernah membahas tentang manajemen risiko teknologi informasi menggunakan ISO 31000:2018, diantaranya ialah penelitian yang berjudul "*Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000*" yang dilakukan oleh Miftakhatun pada tahun 2020, di mana penelitian ini bertujuan untuk mengetahui kemungkinan munculnya risiko dan cara pencegahan maupun penanganan untuk meminimalisir risiko di kemudian hari yang berkaitan dengan proses bisnis utama di dalam *website* Ecofo. Dari penelitian tersebut, teridentifikasi 24 kemungkinan risiko di mana terdapat 3 risiko dengan tingkat risiko *high*, 10 risiko dengan tingkat risiko *medium*, dan 11 risiko dengan tingkatan risiko *low* yang dapat dijadikan acuan pencegahan, penanganan dan pemeliharaan terhadap aset teknologi informasi di masa mendatang [15].

Penelitian selanjutnya berjudul "*Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga*" yang dilakukan oleh Muhammad Ilham Fachrezi dkk. pada tahun 2019 yang mana teknologi informasi berkaitan erat dengan proses bisnis utama sebagai salah satu saran sumber informasi Diskominfo, sehingga penelitian ini bertujuan untuk mengidentifikasi, menganalisis dan mengelola risiko keamanan aset teknologi informasi dan juga mengetahui tingkat risiko pada aspek keamanan aset teknologi informasi. Penelitian menghasilkan temuan bahwa terdapat 2 kemungkinan risiko dengan tingkatan rendah, 11 kemungkinan risiko dengan tingkatan menengah, dan 4 risiko tingkat tinggi [16].

Penelitian yang dilakukan Kwee May Linda Lole pada tahun 2022 dengan judul "*Analisis Manajemen Risiko Pada Aplikasi Pegadaian Digital Service Menu Tabungan Emas Menggunakan ISO 31000:2018*" yang bertujuan untuk menganalisa manajemen risiko teknologi informasi pada implementasi aplikasi Pegadaian Digital Service (PDS) menu tabungan emas di PT Pegadaian Cabang Waingapu dengan menggunakan *framework* ISO 31000:2018. Ditemukan bahwa terdapat 23 kemungkinan risiko yang ada pada aplikasi PDS menu tabungan emas. Dari 23 kemungkinan risiko, ada satu risiko yang berada pada level risiko tinggi, yaitu kebocoran data, enam risiko pada level menengah dan 16 risiko pada level rendah [17].

Penelitian yang dilakukan Diky Yudha Andika dan Agustinus Fritz Wijaya pada tahun 2022 yang berjudul "*Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2018 Pada PT Trust Lerinvital Timur*" di mana tujuan penelitian ini adalah untuk membantu perusahaan dalam hal manajemen risiko, seperti meminimalisir risiko, serta kemungkinan-kemungkinan risiko, dan juga memberikan rekomendasi yang tepat bagi PT Trust Lerinvital Timur terhadap risiko risiko yang telah diidentifikasi maupun risiko-risiko yang sewaktu-waktu dapat muncul membahayakan sistem kerja ERP perusahaan. Dari penelitian tersebut, ditemukan bahwa terdapat 26 risiko yang menghambat kinerja dari proses bisnis yang berjalan di PT Trust Lerinvital Timur. Berdasarkan penelitian ini, sudah ditemukan 3 risiko yang masuk dalam tingkatan *high*, seperti *server down*, *web service* yang sering mati, dan juga koneksi jaringan yang sering terputus. Selain itu juga terdapat 13 risiko dengan klasifikasi *medium*, yang meliputi kegagalan *software*, sistem *crash*, *human error*, koneksi jaringan tidak stabil, gempa bumi, petir, kerusakan *hardware*, proses *maintenance* tidak terjadwal, *overload*, serta *data corrupt*. Dan juga terdapat 10 risiko dengan tingkatan *low*, seperti penyalahgunaan hak akses, *overheat*, *overcapacity*, banjir, *cybercrime*, serangan virus, vandalisme, kegagalan *backup*, serta memori penuh. Dari risiko-risiko tersebut, peneliti tersebut memberikan rekomendasi-rekomendasi penanganan risiko yang diharapkan dan sekiranya dapat diterapkan oleh PT Trust Lerinvital Timur, seperti mengganti ISP terbaru, melakukan *troubleshooting* ketika *web service* mati, serta melakukan pengecekan berkala pada *database*, sehingga proses bisnis perusahaan dapat terus berjalan dengan baik [18].

Lalu, terdapat satu penelitian lagi di tahun 2009 yang dilakukan oleh Anandhi Bharadwaj, Mark Keil, Magnus Mähring dengan judul "*Effects of information technology failures on the market value of firms*" Dari penelitian tersebut, peneliti mengaitkan kegagalan teknologi informasi terhadap nilai pasar perusahaan, dan ditemukan bahwa, dari 213 sampel laporan surat kabar tentang kegagalan teknologi informasi perusahaan publik 10 tahun terakhir, menunjukkan bahwa kegagalan teknologi informasi menghasilkan rata-rata 2% penurunan abnormal kumulatif pada harga saham selama 2 hari. Hasil juga mengungkapkan bahwa pasar merespon lebih negatif terhadap kegagalan implementasi yang mempengaruhi sistem baru daripada kegagalan operasi yang melibatkan sistem saat ini. Selanjutnya, penelitian ini

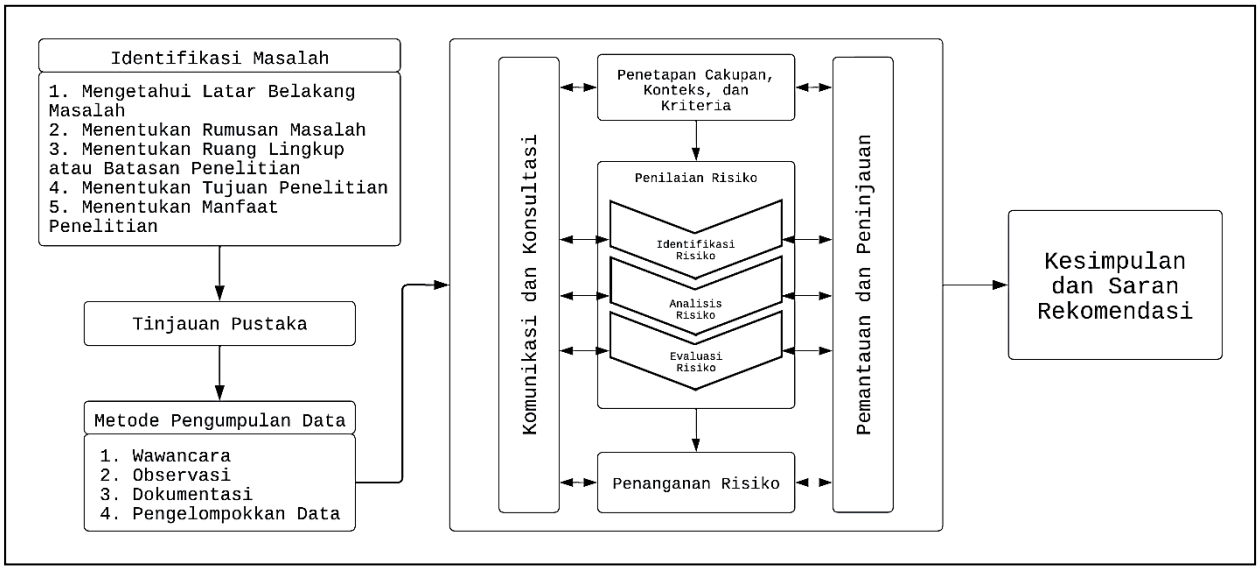
menunjukkan bahwa kegagalan teknologi informasi yang lebih parah mengakibatkan penurunan nilai perusahaan yang lebih besar dan bahwa perusahaan dengan riwayat kegagalan teknologi informasi mengalami dampak negatif yang lebih besar [19].

Berdasarkan data serta hasil penelitian di atas, penulis menyimpulkan bahwa setiap perusahaan tentu memiliki risiko-risiko yang menimpa teknologi informasi, entah sudah diketahui maupun belum diketahui, serta kegagalan teknologi informasi yang ternyata juga merusak nama baik perusahaan dan menjatuhkan nilai perusahaan itu sendiri. Oleh karena itu, penulis tertarik untuk melakukan penelitian manajemen risiko teknologi informasi menggunakan *framework* ISO 31000:2018 dengan tujuan untuk mengetahui, menilai, dan meminimalisir risiko yang ada dalam perusahaan, sehingga penelitian ini dapat bermanfaat bagi perusahaan.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Berikut merupakan alur tahapan atau *flowchart* yang menggambarkan tahapan-tahapan dalam melakukan sebuah penelitian manajemen risiko dengan *framework* ISO 31000:2018, di mana tahapan-tahapan tersebut harus diikuti agar mampu memahami masalah yang ada, mendapatkan data yang akurat, serta menghasilkan hasil analisis yang tepat, jelas, dan berguna.



Gambar 1. Tahapan Penelitian ISO 31000 [20]

Penelitian yang dilakukan merupakan penelitian yang bersifat kualitatif agar mendapatkan data yang mendalam dan teliti demi memahami permasalahan atau fenomena yang terjadi. Metode penelitian ini memiliki tahapan-tahapan sebagai berikut:

a. Identifikasi Masalah

Merupakan tahapan pertama dalam melaksanakan penelitian yang terdiri atas: Mengetahui latar belakang masalah, menentukan rumusan masalah, menentukan ruang lingkup atau batasan penelitian, menentukan tujuan penelitian, dan menentukan manfaat dari penelitian di mana identifikasi masalah bertujuan agar peneliti memahami penerapan *Framework* ISO 31000:2018 sebagai sarana dalam menganalisis risiko serta memahami objek studi kasus yang akan diteliti.

b. Tinjauan Pustaka

Tinjauan Pustaka penting karena bertujuan untuk memahami penelitian yang akan dilakukan, serta membantu peneliti memperkuat adanya sebuah penelitian yang akan dilaksanakan.

c. Metode Pengumpulan Data

Pengumpulan data dapat dilakukan melalui serangkaian metode, yaitu: wawancara terhadap narasumber dari PT XYZ Bawen, observasi terhadap objek studi kasus dengan mendatangi PT XYZ Bawen, dan melakukan dokumentasi wawancara dan observasi. Setelah itu melakukan pengelompokkan data dari hasil wawancara dan observasi.

d. *Framework* ISO 31000:2018

1. Komunikasi dan Konsultasi

   Peneliti melakukan komunikasi dan konsultasi dengan pihak perusahaan dengan tujuan untuk menyamakan persepsi tentang risiko yang akan diidentifikasi, dianalisis, dan dievaluasi, serta mengetahui kesepakatan-kesepakatan yang berkaitan dengan kerahasiaan perusahaan, serta privasi dari setiap individu yang terlibat dalam penelitian.

2. Penetapan Cakupan, Konteks, dan Kriteria
   Cakupan ditentukan untuk memperjelas objek yang akan diteliti, mengetahui sumber yang diperlukan, serta yang bersedia mengetahui siapa yang bertanggung jawab di dalam objek studi kasus. Cakupan dalam penelitian ini yaitu berkaitan dengan manajemen risiko teknologi informasi pada PT XYZ cabang Bawen dengan menggunakan *framework* ISO 31000:2018.

   Lalu, konteks yang ditetapkan dalam penelitian ini, yaitu mengetahui secara pasti risiko-risiko yang ada dalam perusahaan, apakah teknologi informasi yang ada berjalan dengan semestinya atau justru menghambat proses bisnis dan tujuan perusahaan. Untuk memetakan risiko tersebut, kriteria-kriteria risiko disusun yang terdiri dari kriteria *likelihood* dan *impact* dalam menentukan tingkat risiko. *Likelihood* merupakan frekuensi dari terjadinya risiko dan *impact* merupakan nilai dampak yang terjadi pada risiko.
3. Penilaian Risiko
   a) Identifikasi Risiko
      Pada tahap ini, peneliti melakukan identifikasi risiko dengan terlebih dahulu mengetahui seluruh aset teknologi informasi PT XYZ Bawen, sehingga peneliti dapat memahami dan menentukan kemungkinan risiko yang paling mungkin terjadi terhadap aset-aset tertentu yang dimiliki perusahaan.
   b) Analisis Risiko
      Pada tahap ini, risiko-risiko yang diidentifikasi akan dianalisis untuk menentukan nilai *likelihood* dan *impact* yang disebabkan dari risiko yang telah ditemukan dari hasil identifikasi kemungkinan risiko di mana hasil analisis akan memberikan dasar pemahamanan dalam pengambilan keputusan terhadap penangan risiko.
   c) Evaluasi Risiko
      Pada tahap evaluasi, evaluasi risiko membantu peneliti dan perusahaan dalam proses pengambilan keputusan terhadap penangan risiko dengan melakukan pemetaan risiko berdasarkan hasil perbandingan nilai kriteria *likelihood* dan *impact*.
4. Penanganan Risiko
   Berdasarkan seluruh hasil akhir penilaian risiko, maka pada tahap ini merupakan tahap di mana saran atau rekomendasi penanggulangan dan atau peminimalisiran risiko diberikan yang dimulai dari risiko dengan tingkatan tertinggi.
5. Pemantauan dan Peninjauan
   Pemantauan dan peninjauan terhadap saran atau rekomendasi yang diberikan, dilakukan dengan komunikasi serta penyerahan laporan penelitian kepada dosen pembimbing peneliti dan kepada perusahaan.
6. Kesimpulan dan Saran Rekomendasi
   Setelah dosen pembimbing dan perusahaan telah menyetujui laporan penelitian, penelitian akan memiliki kesimpulan yang jelas terhadap hasil penelitian. Saran bagi perusahaan juga akan ditegaskan di dalam laporan penelitian, begitu juga saran rekomendasi bagi para peneliti selanjutnya tentang apa saja peluang penelitian selanjutnya pada topik penelitian yang sama.

3. HASIL DAN PEMBAHASAN

3.1 Komunikasi dan Konsultasi

Komunikasi dan konsultasi menjadi tahapan awal dalam melaksanakan manajemen risiko berdasarkan framework ISO 31000:2018 dengan menyamakan pemahaman dan persepsi tentang manajamen risiko dan risiko dengan pihak PT XYZ Bawen, terkhususnya bersama dengan divisi IT. Tahap ini juga menjadi tahap awal dalam mengumpulkan data ataupun informasi yang berkaitan dengan profil bisnis perusahaan, serta data risiko yang nantinya akan diidentifikasi, dianalisis, dan dievaluasi secara mendalam.

3.2 Cakupan, Konteks, dan Kriteria

Cakupan atau *scope* dalam penelitian ini yaitu manajemen risiko teknologi informasi pada PT XYZ cabang Bawen dengan menggunakan *framework* ISO 31000:2018, dengan konteks tujuan untuk mengetahui risiko-risiko teknologi informasi yang dimiliki perusahaan saat ini, apakah berjalan sesuai keinginan perusahaan atau berjalan dengan tidak maksimal dan menghambat perusahaan mencapai tujuan bisnisnya. Cakupan dan konteks dapat mulai ditindaklanjuti dengan penetapan dan penentuan kriteria risiko berdasarkan frekuensi kejadiannya (*likelihood*) dan berdasarkan dampak risiko (*impact*) terhadap perusahaan.

Likelihood terbentuk atas 5 kriteria, yaitu *Rare*, *Unlikely*, *Possible*, *Likely*, dan *Certain*, seperti yang dapat dilihat pada Tabel 1, yang mana setiap kriteria tersebut menunjukkan frekuensi waktu kejadian dari risiko-risiko yang ada. Lalu, *Impact* terbentuk atas 5 kriteria, yaitu *Insignificant*, *Minor*, *Moderate*, *Major*, dan *Catastrophic*, seperti yang dapat dilihat pada Tabel 2 yang menunjukkan tingkat dampak bahaya dari risiko-risiko yang ditemukan.

Tabel 1. Kriteria *Likelihood*

Kriteria	Keterangan	Frekuensi	Nilai
Rare	Risiko sangat jarang terjadi	> 3 tahun	1

Unlikely	Risiko jarang terjadi	2-3 tahun	2
Possible	Risiko kadang terjadi	1-2 tahun	3
Likely	Risiko sering terjadi	7-12 bulan	4
Certain	Risiko pasti terjadi	< 7 bulan	5

Tabel 2. Kriteria *Impact*

Kriteria	Keterangan	Nilai
Insignificant	Risiko tidak menggangu aktivitas operasional perusahaan.	1
Minor	Risiko dapat menghambat aktivitas perusahaan, namun tidak menghambat aktivitas utama perusahaan.	2
Moderate	Risiko menghambat jalannya proses bisnis yang mengakibatkan terganggunya sebagian besar aktifitas perusahaan.	3
Major	Risiko menyebabkan hambatan pada hampir seluruh aktifitas perusahaan.	4
Catastrophic	Risiko menyebabkan seluruh aktivitas perusahaan berhenti total.	5

Selanjutnya, matriks evaluasi akan dibentuk berdasarkan kriteria *Likelihood* dan *Impact* yang telah ditetapkan, dengan tujuan untuk memetakan risiko yang ada dengan membagi risiko menjadi 3 tingkatan, yaitu *low*, *medium*, dan *high* untuk mengetahui risiko mana yang harus lebih dahulu ditindaklanjuti. Perhatikan Tabel 3 dan Tabel 4 di bawah ini.

Tabel 3. Matriks Evaluasi Risiko

Likelihood						
	Certain	**5**	**10**	**15**	**20**	**25**
	Likely	**4**	**8**	**12**	**16**	**20**
	Possible	**3**	**6**	**9**	**12**	**15**
	Unlikely	**2**	**4**	**6**	**8**	**10**
	Rare	**1**	**2**	**3**	**4**	**5**
Matriks Evaluasi		*Insignificant*	*Minor*	*Moderate*	*Major*	*Catastrophic*
		Impact				

Tabel 4. Keterangan Warna Risiko

Warna	Jenis Risiko	Keterangan Risiko
	Low Risk	Risiko dengan pengaruh kecil terhadap perusahaan, dapat diatasi dengan menerapkan kebijakan tertentu**.**
	Medium Risk	Risiko mampu menyebabkan sedikit gangguan dalam bisnis, dapat diatasi dengan menerapkan kebijakan tertentu yang disertai dengan pengawasan**.**
	Medium High Risk	Risiko menyebabkan cukup gangguan yang dapat merugikan, sehingga memerlukan pengawasan dan membutuhkan penanganan
	High Risk	Risiko berbahaya dan sangat merugikan, harus segera diatasi secepatnya.

3.3 Penilaian Risiko

Penilaian Risiko terhadap PT XYZ cabang Bawen dibagi menjadi tiga tahapan, yaitu identifikasi kemungkinan-kemungkinan risiko yang dapat terjadi, analisis risiko dengan merujuk pada kriteria *likelihood* dan *impact*, dan evaluasi risiko dengan matriks evaluasi risiko.

3.3.1 Identifikasi Risiko

Identifikasi risiko menjadi tahap pertama dalam penilaian risiko untuk mengetahui berbagai kemungkinan risiko yang dapat terjadi yang mempengaruhi aset-aset dan aktivitas dalam perusahaan. Oleh karena itu, identifikasi risiko dibagi menjadi dua tahapan identifikasi: 1) identifikasi aset dan 2) identifikasi kemungkinan risiko. Tahapan identifikasi aset akan berguna dalam menentukan kemungkinan risiko yang terjadi apabila aset-aset yang ada dalam perusahaan mengalami sebuah gangguan.

3.3.1.1 Identifikasi Aset

Aset yang akan diidentifikasi dibagi dalam 3 kelompok atau kategori aset, yaitu aset Data, aset software, dan aset hardware milik perusahaan. Identifikasi aset diperlukan agar kemungkinan risiko dapat diidentifikasi sesuai dengan risiko yang berkaitan dengan penggunaan aset-aset tersebut.

Tabel 5. Aset PT XYZ Bawen

Kategori Aset	Daftar Aset
Data	Data Logistik
	Data Produksi
	Data Marketing

	Data Customer
	Data Akuntasi
	Data Human Resource
Software	SAP ERP
	Microsoft Office
	Aplikasi Logistik
	Aplikasi Salesman
	Aplikasi Design
	Aplikasi HR
Hardware	Komputer
	Server
	Router
	Hub
	Switch
	LAN CAT6
	Printer
	Telepon
	Scanner
	UPS
	Genset

Aset-aset dalam tabel 5 merupakan keseluruhan aset TI yang penting bagi PT XYZ, di mana terdapat 6 jenis aset data penting, lalu terdapat 6 *software* yang berkaitan dengan operasional manajemen (SAP ERP), operasional kantor (Microsoft Office), operasional penjualan (Aplikasi Logistik dan Aplikasi Salesman), operasional sumber daya (Aplikasi HR), dan operasional desain produk (Aplikasi Desain). Lalu, untuk aset *hardware* merupakan aset-aset TI utama kantor yang berkaitan dengan berjalannya administratif perusahaan.

3.3.1.2 Identifikasi Kemungkinan Risiko

Setelah aset-aset penting perusahaan teridentifikasi, maka kemungkinan risiko yang dapat mengancam atau mengganggu pemanfaatan aset dapat lebih mudah untuk dikenali. Risiko yang dapat mengancam perusahaan dapat dipengaruhi oleh berbagai faktor. Terdapat 3 faktor utama munculnya sebuah risiko, diantaranya ialah karena faktor alam dan lingkungan, faktor kualitas/kuantitas sumber daya manusia, dan faktor sistem, infrastruktur, dan data yang digunakan perusahaan.

Tabel 6. Identifikasi Kemungkinan dan Dampak Risiko yang dapat terjadi di PT XYZ Bawen

Faktor Risiko	ID Risiko	Risiko	Dampak Risiko
Alam & Lingkungan	AL1	Banjir	Kerusakan aset-aset TI dan material produksi, menyebabkan gangguan pada hampir seluruh aktivitas perusahaan.
	AL2	Tanah Longsor	Kerusakan gedung dan aset perusahaan, korban jiwa, hampir seluruh aktivitas perusahaan terhenti.
	AL3	Gempa Bumi	Kerusakan gedung dan aset perusahaan, korban jiwa, seluruh aktivitas perusahaan berhenti.
	AL4	Gunung Meletus	Kerusakan gedung dan aset perusahaan, korban jiwa, seluruh aktivitas perusahaan berhenti.
	AL5	Kebakaran	Kerusakan gedung dan aset perusahaan, korban jiwa, seluruh aktivitas perusahaan berhenti.
	AL6	Angin Topan	Kerusakan gedung dan sebagian aset perusahaan, korban jiwa, hampir seluruh aktivitas perusahaan berhenti.
Sumber Daya Manusia	HR1	Penyalahgunaan Hak Akses Sistem	Memungkinkan terjadinya kebocoran data dan adanya tindakan manipulasi data, serta manipulasi konfigurasi sistem yang sudah ada.
	HR2	Ketidakpahaman Pegawai tentang Penggunaan Perangkat TI	Proses bisnis tertentu dapat terhambat apabila proses bisnis tersebut memang memerlukan bantuan *software*/*hardware* TI.
	HR3	Penyalahgunaan Aset Perusahaan oleh Pegawai/Mantan Pegawai	Kebocoran data dan rahasia penting perusahaan, memperburuk citra perusahaan, serta kerugian finansial.
	HR4	Kekurangan Staff TI	Tidak adanya pengawasan terhadap proses berjalannya SI/TI, jika terjadi kerusakan ataupun

			gangguan, tidak bisa segera ditindaklanjuti akibat kurangnya jumlah Staff TI.
	HR5	Rendahnya Kualitas Staff TI	Jika terjadi kerusakan ataupun gangguan pada SI/TI, tidak bisa segera ditindaklanjuti akibat kualitas Staff TI tidak sesuai harapan.
Sistem, Infrastruktur, dan Data	SID1	Gangguan Koneksi Internet	Tidak bisa mengakses ERP atau aplikasi bisnis lainnya yang memerlukan internet, menyebabkan terganggunya sebagian aktifitas perusahaan.
	SID2	Malfungsi atau Disfungsi *Server*	Kehilangan data-data penting perusahaan.
	SID3	*Hardware Overheat* pada *Rack Server*, Komputer, Laptop, *Router*, *Hub*, *Switch*	Kinerja *hardware* berkurang, bila tidak segera ditangani dapat menyebabkan kerusakan pada aset *hardware* akibat panas berlebih, menyebabkan akses terhadap aplikasi TI terhambat, kehilangan data, serta kehilangan akses internet.
	SID4	Pencurian *Hardware*	Proses bisnis tertentu dapat terhambat apabila proses bisnis tersebut memang memerlukan bantuan *hardware* TI, serta kerugian finansial apabila harus membeli *hardware* TI yang baru.
	SID5	Malfungsi atau Disfungsi *Hardware*	Proses bisnis tertentu dapat terhambat apabila proses bisnis tersebut memang memerlukan bantuan *hardware* TI, serta kerugian finansial apabila harus membeli *hardware* TI yang baru apabila *hardware* diketahui telah mengalami kerusakan permanen.
	SID6	*Data Storage* Penuh	Tidak dapat menambah atau menyimpan data-data terbaru milik perusahaan.
	SID7	Pencurian Data	Kebocoran data dan rahasia penting perusahaan, serta memperburuk citra perusahaan.
	SID8	Kegagalan *Data Backup*	Risiko kehilangan data-data perusahaan meningkat.
	SID9	*Data Corrupt*	Kehilangan data-data penting perusahaan.
	SID10	Aplikasi Perusahaan Tidak Dapat Diakses	Pembuatan dokumen, penginputan data, akses terhadap E-mail yang mana memerlukan penggunaan aplikasi menjadi tak dapat dilakukan, menyebabkan gangguan pada proses administratif perusahaan.
	SID11	*Cybercrime* (*Virus*, *Malware*, *Trojan*, *Cracking*)	Kehilangan data dan atau kebocoran data yang dapat memperburuk citra perusahaan dan kerugian finansial karena harus mengeluarkan biaya dalam mereparasi *hardware* atau bahkan membeli *hardware* baru.
	SID12	Perawatan Sistem dan Infrastruktur Tidak Terlaksana	Risiko kerusakan terhadap aset-aset TI dapat meningkat.
	SID13	Pemadaman Listrik	Terhentinya seluruh aktifitas perusahaan, terutama pada bagian produksi. Pada bagian TI, risiko kerusakan pada *HDD* komputer meningkat, risiko *data corrupt* meningkat.
	SID14	Kurangnya Inovasi Teknologi Perusahaan	Sistem dan infrastruktur TI tertinggal dan rentan terhadap *cybercrime*.
	SID15	Dokumentasi Sistem Tidak Maksimal (contoh: Dokumentasi manual sistem, dokumentasi *maintenance*, dokumentasi *user acceptance*, dokumentasi penerapan sistem, dokumentasi kerusakan, dan sejenisnya)	Meningkatkan risiko akan kerusakan sistem dan infrastruktur karena tidak adanya dokumentasi tentang penggunaan yang tepat, perawatan (*maintenance*), kerusakan, dan bagaimana cara memperbaikinya, serta memperlambat kinerja pegawai dalam hal efisiensi penggunaan sistem.

Di dalam tabel 6, terdapat macam-macam kemungkinan risiko berjumlah 26 jenis kemungkinan risiko yang dapat mengancam dan merugikan pihak PT XYZ bila terjadi, sehingga kemungkinan-kemungkinan risiko tersebut perlu dipertimbangkan dan diwaspadai dengan seksama.

3.3.2 Analisis Risiko

Analisis Risiko dilakukan untuk menilai risiko yang ditemukan pada PT XYZ Bawen berdasarkan nilai *Likelihood* dan *Impact*. Penilaian tersebut dapat dilihat pada tabel 7 berikut ini.

Tabel 7. Penilaian Risiko

Faktor Risiko	ID Risiko	Risiko	*Likelihood*	*Impact*	*Nilai Risiko*
Alam & Lingkungan	AL1	Banjir	1	4	4
	AL2	Tanah Longsor	1	4	4
	AL3	Gempa Bumi	1	4	4
	AL4	Gunung Meletus	1	4	4
	AL5	Kebakaran	1	4	4
	AL6	Angin Topan	1	4	4
Sumber Daya Manusia	HR1	Penyalahgunaan Hak Akses Sistem	1	4	4
	HR2	Ketidakpahaman Pegawai tentang Penggunaan Perangkat TI	5	1	5
	HR3	Penyalahgunaan Aset Perusahaan oleh Pegawai/Mantan Pegawai	3	4	12
	HR4	Kekurangan Staff TI	3	3	9
	HR5	Rendahnya Kualitas Staff TI	1	3	3
Sistem, Infrastruktur, dan Data	SID1	Gangguan Koneksi Internet	3	3	9
	SID2	Malfungsi atau Disfungsi *Server*	3	4	12
	SID3	*Hardware Overheat* pada *Rack Server*, Komputer, Laptop, *Router*, *Hub*, *Switch*	2	4	8
	SID4	Pencurian *Hardware*	1	4	4
	SID5	Malfungsi atau Disfungsi *Hardware*	3	3	9
	SID6	*Data Storage* Penuh	2	3	6
	SID7	Pencurian Data	1	4	4
	SID8	Kegagalan *Data Backup*	2	3	6
	SID9	*Data Corrupt*	2	4	8
	SID10	Aplikasi Perusahaan Tidak Dapat Diakses	3	5	15
	SID11	*Cybercrime* (*Virus*, *Malware*, *Trojan*, *Cracking*)	1	4	4
	SID12	Perawatan Sistem dan Infrastruktur Tidak Terlaksana	1	3	3
	SID13	Pemadaman Listrik	1	4	4
	SID14	Kurangnya Inovasi Teknologi Perusahaan	1	3	3
	SID15	Dokumentasi Sistem Tidak Maksimal (contoh: Dokumentasi manual sistem, dokumentasi *maintenance*, dokumentasi *user acceptance*, dokumentasi penerapan sistem, dokumentasi kerusakan, dan sejenisnya)	1	4	4

Dalam tabel 7, terdapat beberapa risiko yang perlu diwaspadai oleh perusahaan, diantaranya ialah risiko-risiko tingkat *medium high* hingga *high*, yaitu HR3, HR4, SID1, SID2, SID5, dan SID10, di mana faktor risiko Sistem, Infrastruktur, dan Data menjadi faktor yang harus diperhatikan oleh perusahaan, karena proses bisnis PT XYZ juga bergantung terhadap sistem dan infrastruktur TI, serta juga menjadikan data sebagai komponen penting perusahaan yang harus diamankan dan digunakan sebaik dan seefisien mungkin.

3.3.3 Evaluasi Risiko

Evaluasi Risiko menjadi tahap akhir Penilaian Risiko dengan memetakan risiko berdasarkan nilai risiko yang telah dianalisis dengan matriks evaluasi risiko. Matriks evaluasi risiko dapat dilihat pada Tabel 8 seperti berikut.

Tabel 8. Pemetaan Risiko menggunakan Matriks Evaluasi Risiko

Likelihood						
	Certain	**5 (HR2)**	**10**	**15**	**20**	**25**
	Likely	**4**	**8**	**12**	**16**	**20**
	Possible	**3**	**6**	**9 (HR4, SID1, SID5)**	**12 (HR3, SID2)**	**15 (SID10)**
	Unlikely	**2**	**4**	**6 (SID6, SID8)**	**8 (SID3, SID9)**	**10**
	Rare	**1**	**2**	**3 (HR5, SID12, SID14)**	**4 (AL1, AL2, AL3, AL4, AL5, AL6, HR1, SID4, SID7, SID11, SID13, SID15)**	**5**

Matriks Evaluasi	*Insignificant*	*Minor*	*Moderate*	*Major*	*Catastrophic*

Berdasarkan pemetaan risiko pada tabel 8, risiko-risiko tersebar ke berbagai tingkatan risiko, di mana terdapat 15 risiko berada pada tingkatan *low*, 5 risiko berada pada tingkatan *medium*, 5 risiko berada pada tingkatan *medium high*, dan 1 risiko berada pada tingkatan *high*.

3.4 Penanganan Risiko

Penanganan risiko didasari pada hasil penilaian risiko yang dapat dilihat melalui matriks evaluasi risiko (Tabel 8). Tahap penanganan risiko dilakukan dengan pemberian saran/rekomendasi penanganan risiko oleh peneliti dengan harapan risiko dapat ditangani ataupun diminimalisir yang dapat dilihat pada tabel 9.

Tabel 9. Rekomendasi Penanganan Risiko

ID Risiko	Risiko	Tingkat Risiko	Saran Penanganan Risiko
SID10	Aplikasi Perusahaan Tidak Dapat Diakses	High (15)	Segera melapor kepada bagian TI perusahaan, agar bagian TI segera melakukan pemeriksaan lebih lanjut terhadap aplikasi yang bermasalah, serta reparasi secara menyeluruh dan tepat.
HR3	Penyalahgunaan Aset Perusahaan oleh Pegawai/Mantan Pegawai	Medium High (12)	Menerapkan pembatasan hak akses bagi pegawai, terutama bila aset tersebut bukanlah aset utama dari divisi pegawai tersebut.
SID2	Malfungsi atau Disfungsi *Server*	Medium High (12)	Melapor kepada bagian TI perusahaan, agar bagian TI segera melakukan pemeriksaan dan reparasi.
HR4	Kekurangan Staff TI	Medium High (9)	Melakukan perekrutan untuk lowongan yang berkaitan dengan TI secara ketat dan tepat, agar mendapatkan pegawai staff TI yang kompeten sesuai standar perusahaan.
SID1	Gangguan Koneksi Internet	Medium High (9)	Menghubungi pihak penyedia layanan internet (ISP) untuk mengetahui permasalahan yang dialami, serta meminta perbaikan koneksi internet segera.
SID5	Malfungsi atau Disfungsi *Hardware*	Medium High (9)	Melapor kepada bagian TI perusahaan, agar bagian TI segera melakukan pemeriksaan dan reparasi.
SID3	*Hardware Overheat* pada *Rack Server*, Komputer, Laptop, *Router*, *Hub*, *Switch*	Medium (8)	Melakukan pengecekan terhadap kualitas pendingin ruangan untuk *rack server*, *router*, *hub*, *dan switch*. Lalu melakukan pengecekan *heatsink fan* pada komputer dan laptop, serta mengganti *thermal paste*.
SID9	*Data Corrupt*	Medium (8)	*Data corrupt* disebabkan oleh berbagai hal yang berkaitan dengan kegagalan terhadap pembuatan, perubahan, dan penghapusan data, sehingga diharuskan berhati-hati dalam melakukan pembuatan, perubahan, dan penghapusan data, serta melakukan *data backup* secara berkala.
SID6	*Data Storage* Penuh	Medium (6)	Selalu menyiapkan *harddisk* cadangan, serta meningkatkan kapasitas *cloud storage* agar penambahan data tidak terhambat akibat *data storage* yang penuh. Lalu, melakukan pengecekan jumlah kapasitas penyimpanan secara berkala oleh masing-masing *device user*.
SID8	Kegagalan *Data Backup*	Medium (6)	Melakukan pembuatan *system restore point* untuk mengantisipasi kegagalan *data backup* apabila kegagalan tersebut menyebabkan kegagalan sistem. Serta tetap melakukan *data backup* secara berkala.
HR2	Ketidakpahaman Pegawai tentang Penggunaan Perangkat TI	Medium (5)	Melakukan pelatihan penggunaan perangkat TI agar pegawai dapat menggunakan perangkat dengan lancar sesuai SOP perusahaan tanpa mengganggu proses bisnis perusahaan.

Melalui tabel 9, dapat dilihat bahwa rekomendasi diberikan terutama pada risiko-risiko dari tingkat *medium* hingga *high* dengan tujuan untuk lebih memperhatikan risiko-risiko yang mampu mengganggu proses berjalannya bisnis dalam perusahaan dan diharapkan mampu meminimalisir dan mencegah kemungkinan terjadinya lagi risiko tersebut.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan pada PT XYZ Bawen menggunakan *framework* ISO 31000:2018, didapatkan hasil analisis manajemen risiko, di mana dari 26 kemungkinan risiko, terdapat 15 risiko dengan tingkat risiko rendah (*low*), yaitu banjir (AL1), tanah longsor (AL2), gempa bumi (AL3), gunung meletus (AL4), kebakaran (AL5), angin

topan (AL6), penyalahgunaan hak akses sistem (HR1), rendahnya kualitas staff TI (HR5), pencurian *hardware* (SID4), pencurian data (SID7), *Cybercrime* meliputi *virus, malware, trojan* hingga *cracking* (SID11), perawatan sistem dan infrastruktur tidak terlaksana (SID12), pemadam listrik (SID13), kurangnya inovasi teknologi perusahaan (SID14), dan dokumentasi sistem yang tidak maksimal (SID15), 5 risiko dengan tingkat risiko menengah (*medium*), yaitu ketidakpahaman pegawai tentang penggunaan perangkat TI (HR2), *hardware overheat* pada *rack server*, komputer, laptop, *router, hub*, dan *switch* (SID3), *data storage* penuh (SID6), kegagalan *data backup* (SID8), *data corrupt* (SID9), 5 risiko dengan tingkat risiko menengah tinggi (*medium high*), yaitu penyalahgunaan aset perusahaan oleh pegawai/mantan pegawai (HR3), kekurangan staff TI (HR4), gangguan koneksi internet (SID1), malfungsi atau disfungsi *server* (SID2), dan malfungsi atau disfungsi *hardware* (SID5), dan 1 risiko dengan tingkat risiko tinggi (*high*), yaitu aplikasi perusahaan tidak dapat diakses (SID10). Dari risiko-risiko tersebut, perusahaan diharapkan untuk mewaspadai risiko-risiko dari tingkat *medium* hingga *high*, sehingga terdapat saran-saran rekomendasi yang diberikan bagi risiko-risiko ditingkatan tersebut (tabel 9) yang dapat perusahaan lakukan untuk mencegah kerugian yang sekiranya dapat terjadi di masa depan. Lalu, saran untuk penelitian selanjutnya, penelitian yang dilakukan ini terbatas pada analisa manajemen risiko teknologi informasi berdasarkan *framework* ISO 31000:2018, perlu adanya kajian lebih lanjut tentang manajemen risiko yang tidak hanya terbatas pada lingkup teknologi informasi dan *framework* ISO 31000:2018, dengan tujuan untuk memaksimalkan pencegahan risiko pada lingkup bagian lain dari perusahaan, sehingga perusahaan dapat merasakan manfaat yang maksimal terhadap penelitian-penelitian manajemen risiko melalui penerapan berbagai *framework* lainnya, serta tidak hanya pada ranah teknologi informasi saja.

REFERENCES

[1] Daryanto Setiawan, "Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya Impact of Information Technology Development and Communication on," *J. Pendidik.*, vol. X, no. 2, pp. 195–211, 2017.

[2] C. A. Cholik, "Perkembangan Teknologi Informasi Komunikasi / ICT dalam Berbagai Bidang," *J. Fak. Tek. UNISA Kuningan*, vol. 2, no. 2, pp. 39–46, 2021.

[3] S. M. T. Situmeang, "PENYALAHGUNAAN DATA PRIBADI SEBAGAI BENTUK KEJAHATAN SEMPURNA DALAM PERSPEKTIF HUKUM SIBER," *SASI*, vol. 27, no. 1, p. 38, Mar. 2021, doi: 10.47268/sasi.v27i1.394.

[4] I. P. A. E. Pratama and M. T. S. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," *J. Telemat.*, vol. 15, no. 2, pp. 63–70, 2020.

[5] T. Meyer and G. Reniers, *Engineering Risk Management*. De Gruyter, 2022. doi: 10.1515/9783110665338.

[6] A. Rocha, "2019 14th Iberian Conference on Information Systems and Technologies (CISTI) : proceedings of CISTI'2019 - 14th Iberian Conference on Information Systems and Technologies : 19 to 22 of June 2019, Coimbra, Portugal," *14th Iber. Conf. Inf. Syst. Technol.*, no. June, pp. 1–6, 2019.

[7] A. Widyastuti and N. A. N. Zakiyah, "Amanah di Balik Implementasi Manajemen Risiko," *Reviu Akunt. dan Bisnis Indones.*, vol. 5, no. 2, pp. 151–163, Dec. 2021, doi: 10.18196/rabin.v5i2.12966.

[8] E. Sudarmanto, "Manajemen Risiko: Deteksi Dini Upaya Pencegahan Fraud," *J. Ilmu Manaj.*, vol. 9, no. 2, p. 107, Jun. 2020, doi: 10.32502/jimn.v9i2.2506.

[9] S. Tranchard, "The new ISO 31000 keeps risk management simple," *Gov. Dir.*, no. May, pp. 180–183, 2018.

[10] W. Y. Nuswantoro, U. Pembangunan, N. Veteran, J. Timur, and K. Surabaya, "Penerapan Manajemen Risiko Berbasis Aset Sebagai Salah Satu Bentuk Pengamanan Perusahaan pada PT . XYZ," *J. Manaj.*, vol. 2, no. 1, pp. 93–102, 2023, doi: 10.55123/mamen.v2i1.1209.

[11] B. Prihartono, G. Audrey, P. Annasthacia, and F. Fahlevi, "KEPENTINGAN BERBASIS PROSES BISNIS PADA PT X," vol. 18, no. 10, pp. 120–129, 2023.

[12] M. M. Sine and E. Maria, "Analisis Manajemen Risiko pada Penerapan Sistem Informasi Pembangunan Daerah (SIPD) Menggunakan IEC/ISO 31010:2019," *Build. Informatics, Technol. Sci.*, vol. 4, no. 1, 2022, doi: 10.47065/bits.v4i1.1531.

[13] S. A. Atmojo and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 3, pp. 546–558, 2020, doi: 10.35957/jatisi.v7i3.525.

[14] W. F. Worotikan and E. Maria, "KLIK: Kajian Ilmiah Informatika dan Komputer Penerapan ISO 31000:2018 untuk Manajemen Risiko E-Ticketing Taman Rekreasi XYZ," *Media Online*, vol. 3, no. 5, pp. 449–456, 2023, [Online]. Available: https://djournals.com/klik

[15] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, Aug. 2020, doi: 10.36596/jcse.v1i2.76.

[16] M. I. Fachrezi, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000:2018 Diskominfo Kota Salatiga," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 2, pp. 764–773, 2021, doi: 10.35957/jatisi.v8i2.789.

[17] K. M. Linda Lole and E. Maria, "Analisis Manajemen Risiko Pada Aplikasi Pegadaian Digital Service Menu Tabungan Emas Menggunakan ISO 31000:2018," *J. Sist. Komput. dan Inform.*, vol. 3, no. 3, p. 319, 2022, doi: 10.30865/json.v3i3.3891.

[18] D. Andika and A. Wijaya, "MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK ISO 31000:2018 PADA PT. TRUST LERINVITAL TIMUR," *J. Mnemon.*, vol. 5, no. 2, pp. 111–118, Aug. 2022, doi: 10.36040/mnemonic.v5i2.4778.

[19] A. Bharadwaj, M. Keil, and M. Mähring, "Effects of information technology failures on the market value of firms," *J. Strateg. Inf. Syst.*, vol. 18, no. 2, pp. 66–79, 2009, doi: 10.1016/j.jsis.2009.04.001.

[20] ISO Standards, "ISO 31000:2018 Risk management – Guidelines. International Organization for Standardization.," *ISO Stand.*, 2018.