ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA PT XYZ

Shafira Khansa Fadiyah, Ilham
Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Ampel
Jl. Ahmad Yani No.177, Jemur Wonosari, Kec. Wonocolo, Surabaya, Indonesia
shafirakhansafadiyah@gmail.com

ABSTRAK

Penelitian ini menganalisis manajemen risiko teknologi informasi di PT XYZ dengan menggunakan standar ISO 31000. Dalam era digital, manajemen risiko menjadi aspek krusial untuk memastikan keberlangsungan organisasi. Penelitian ini bertujuan untuk mengevaluasi efektivitas penerapan ISO 31000 dalam mengidentifikasi, menganalisis, dan merespons risiko yang dihadapi perusahaan. Metode yang digunakan adalah pendekatan kualitatif dengan studi kasus, yang melibatkan identifikasi aset, kemungkinan risiko, dampak risiko, dan analisis risiko. Hasil penelitian menunjukkan bahwa PT XYZ menghadapi berbagai risiko, termasuk kebakaran, pencurian data, dan serangan virus, yang dapat berdampak signifikan terhadap operasional dan reputasi perusahaan. Tindakan mitigasi yang diusulkan, seperti instalasi sistem pemadam kebakaran otomatis dan pelatihan keamanan siber, bertujuan untuk mengurangi dampak dan kemungkinan terjadinya risiko. Penelitian ini diharapkan dapat memberikan kontribusi bagi perusahaan lain dalam menerapkan manajemen risiko teknologi informasi secara efektif, dengan menekankan pentingnya keterlibatan manajemen dalam setiap tahap proses pengelolaan risiko.

Kata kunci : *Manajemen Risiko, Teknologi Informasi, ISO 31000, Mitigasi Risiko.*

1. PENDAHULUAN

Perkembangan teknologi informasi telah menjadi pendorong utama transformasi bisnis di era digital, memberikan kemampuan organisasi untuk mempercepat proses bisnis dan meningkatkan efisiensi operasional [1]. Dalam konteks ini, manajemen risiko teknologi informasi menjadi aspek kritis yang menentukan keberlangsungan organisasi.

Standar ISO 31000 telah diakui secara global sebagai kerangka manajemen risiko yang sistematis dan komprehensif, membantu perusahaan mengidentifikasi, menganalisis, mengevaluasi, dan mengelola risiko yang dihadapi [2]. Dalam konteks teknologi informasi, ISO 31000 membantu perusahaan menghadapi tantangan risiko yang muncul dari penerapan teknologi baru dan isu keamanan informasi [3].

Penelitian sebelumnya menunjukkan bahwa implementasi ISO 31000 dapat meningkatkan kemampuan organisasi dalam menghadapi ketidakpastian dan ancaman di teknologi informasi. Studi kasus seperti PT Trust Lerinvital Timur dan RSUD BLUD X menunjukkan manfaat nyata dari standar ini [4]. Selain itu, keterlibatan manajemen yang kuat dalam manajemen risiko teknologi informasi di sektor swasta meningkatkan keberhasilan mitigasi risiko. Contohnya, PT Bayu Buana Tbk berhasil mengidentifikasi 21 potensi risiko dalam sistem teknologi informasi mereka, di mana keterlibatan manajemen berperan penting selama pandemi Covid-19 [5].

Penelitian lain juga menunjukkan bahwa penerapan ISO 31000 dapat meningkatkan efisiensi dan efektifitas dalam mengelola risiko teknologi informasi, seperti yang dilakukan oleh Layanan Ekspedisi XYZ [6]. Hal serupa juga terlihat di PT Pertamina, di mana tanggung jawab manajemen dalam pengelolaan risiko e-recruitment membantu meminimalkan risiko rekrutmen [7].

Studi ini bertujuan untuk mengevaluasi dan mengkaji implementasi kerangka manajemen risiko pada aspek teknologi informasi di PT XYZ, dengan menggunakan panduan dan metodologi yang diatur dalam standar internasional ISO 31000 sebagai acuan utama dalam proses analisis. Tujuan penelitian ini adalah untuk memahami bagaimana manajemen risiko teknologi informasi di PT XYZ dapat dikelola secara efektif dan berkelanjutan. Kajian ini menyoroti peran penting manajemen dalam membangun budaya manajemen risiko yang berkelanjutan di perusahaan, yang tidak hanya melibatkan analisis risiko teknis, tetapi juga menekankan pada pengelolaan risiko dari perspektif manajemen strategis [8].

Penelitian ini diharapkan dapat memberikan kontribusi baru dalam literatur manajemen risiko teknologi informasi dengan menekankan pentingnya tanggung jawab manajemen dalam memastikan keberhasilan penerapan ISO 31000. Selain itu, hasil dari penelitian ini diharapkan dapat menjadi panduan bagi perusahaan lain yang ingin menerapkan manajemen risiko teknologi informasi secara efektif dengan melibatkan manajemen dalam setiap tahap proses pengelolaan risiko. Dengan demikian, penelitian ini tidak hanya relevan bagi PT XYZ, tetapi juga bagi organisasi lain yang menghadapi tantangan serupa dalam mengelola risiko teknologi informasi di era digital yang semakin kompleks.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian mengenai manajemen risiko teknologi informasi menggunakan standar ISO 31000 telah memberikan wawasan berharga tentang penerapannya di berbagai sektor. Evinia dan Sitokdana menunjukkan

bahwa penerapan ISO 31000 dapat meningkatkan efektivitas manajemen risiko TI dengan menyediakan kerangka kerja yang terstruktur untuk mengidentifikasi dan menangani risiko perusahaan. [9]. Penelitian ini menekankan pentingnya keterlibatan manajemen dalam pengelolaan risiko.

Selanjutnya, Moleong dan Tanaamah menganalisis risiko teknologi informasi pada aplikasi InlisLite di Dinas Kearsipan dan Perpustakaan Provinsi Nusa Tenggara Timur, menemukan bahwa ISO 31000 membantu dalam identifikasi risiko dan merumuskan strategi mitigasi yang efektif, sehingga meningkatkan keandalan sistem informasi pemerintah [10].

Prasetyo, Salsabila, dan Retnani juga melakukan analisis manajemen risiko teknologi informasi di institusi pendidikan tinggi dengan menggabungkan ISO 31000 dan analisis Bow Tie. Hasil penelitian menunjukkan bahwa pendekatan ini memberikan gambaran komprehensif tentang risiko dan langkah mitigasi yang lebih tepat sasaran [11]. Penelitian ini menyoroti pentingnya integrasi berbagai metode dalam manajemen risiko untuk meningkatkan ketahanan organisasi terhadap ancaman.

2.2. Manajemen Risiko

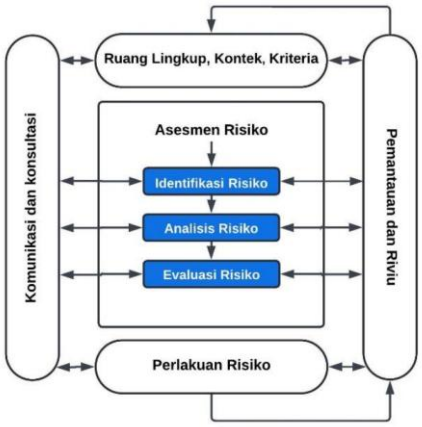
Manajemen risiko merupakan suatu proses berkelanjutan yang melibatkan identifikasi sistematis, analisis mendalam, dan respons terencana terhadap setiap potensi risiko yang dapat menghambat pencapaian target organisasional. Di dalam konteks proyek teknologi informasi, praktik ini memainkan peran strategis dalam memetakan, mengevaluasi, dan mengelola risiko teknologi dan implementasi, sehingga mampu meningkatkan probabilitas keberhasilan proyek dan memitigasi potensi kerugian [12].

2.3. ISO 31000

ISO 31000 adalah standar internasional yang memberikan pedoman untuk manajemen risiko, yang dirancang untuk membantu organisasi dalam mengembangkan kerangka kerja dan proses manajemen risiko yang efektif. Standar ini menekankan pentingnya pendekatan sistematis dalam mengidentifikasi, menganalisis, dan merespons risiko, serta mengintegrasikan manajemen risiko ke dalam semua aspek operasional dan pengambilan keputusan organisasi [13].

3. METODE PENELITIAN

Dengan menggunakan metode kualitatif dan studi literatur, fokus utama penelitian adalah menganalisis penerapan kerangka ISO 31000 dalam mengelola risiko pada sistem teknologi informasi. Analisis dilakukan dengan mengidentifikasi potensi risiko teknologi informasi yang umum dihadapi oleh perusahaan berdasarkan kajian literatur dan best practice dalam industri.



Gambar 1. Tahap Penelitian

Penelitian ini mengikuti kerangka kerja ISO 31000 yang terdiri dari empat tahap utama: identifikasi risiko, analisis risiko, evaluasi risiko, dan perlakuan risiko [14]. Penelitian ini bertujuan untuk memberikan gambaran umum tentang bagaimana kerangka kerja ISO 31000 dapat diterapkan dalam mengelola risiko teknologi informasi di lingkungan perusahaan. Berikut adalah penjelasan dari tahapan kerangka kerja ISO 31000.

Keempat tahapan utamanya dimulai dengan identifikasi risiko, yaitu proses mengidentifikasi dan mendeskripsikan risiko yang dapat mempengaruhi pencapaian tujuan organisasi [5]. Selanjutnya, dilakukan analisis risiko yang merupakan proses memahami karakteristik risiko secara lebih detail untuk menentukan tingkat risiko melalui penilaian kemungkinan dan dampak [15]. Setelah analisis dilakukan, risiko dievaluasi dengan membandingkan hasil analisis risiko terhadap kriteria risiko yang telah ditetapkan untuk menentukan apakah diperlukan perlakuan risiko tambahan [14]. Tahapan yang terakhir adalah perlakuan risiko yang melibatkan pemilihan satu atau lebih opsi penanganan risiko serta implementasinya untuk memodifikasi tingkat risiko menjadi level yang dapat diterima oleh organisasi [16].

4. HASIL DAN PEMBAHASAN

4.1. Identifikasi Aset Risiko

Identifikasi aset adalah langkah pertama untuk memahami elemen-elemen kunci dalam sistem informasi yang perlu dilindungi. Aset tersebut mencakup:

Tabel 1. Tabel Identifikasi Aset

Komponen Sistem Informasi	Aset
Data	Database Perusahaan
	Data Cadangan (Backup)
Software	Seluruh aplikasi yang digunakan perusahaan
	Sistem manajemen lainnya
Hardware	Server
	Komputer Desktop/Laptop
	Perangkat Jaringan

Tabel identifikasi aset mengklasifikasikan komponen sistem informasi menjadi tiga kategori, yaitu data (database perusahaan, dan data cadanagan atau backup), software (seluruh aplikasi yang digunakan perusahaan dan sistem manajemen lainnya), dan hardware (server, computer desktop/laptop, perangkat jaringan).

4.2. Identifikasi Kemungkinan Risiko

Kemungkinan risiko adalah skenario yang dapat menyebabkan kerusakan, kehilangan, atau gangguan terhadap aset yang diidentifikasi. Risiko ini dapat terjadi akibat faktor eksternal seperti bencana alam, atau faktor internal seperti kesalahan manusia dan kegagalan sistem. Beberapa risiko yang teridentifikasi adalah sebagai berikut:

Tabel 2. Tabel Identifikasi Kemungkinan Risiko

ID	Kemungkinan Risiko	Faktor
R01	Debu	Alam
R02	Kebakaran	
R03	Banjir	
R04	Pencurian data seperti hacking	Manusia
R05	Human error	
R06	Penyalahgunaan hak akses	
R07	Kerusakan perangkat keras	Sistem
R08	Serangan virus	
R09	Data hilang	

Tabel identifikasi kemungkinan risiko mengidentifikasi risiko yang dihadapi PT XYZ dalam pengelolaan teknologi informasi, dikelompokkan menjadi tiga kategori: alam (debu, kebakaran, banjir, pencurian data), manusia (kesalahan, pencurian, penyalahgunaan akses, kerusakan perangkat keras), dan sistem (serangan virus, kehilangan data). Identifikasi ini membantu PT XYZ merencanakan langkah mitigasi yang tepat untuk melindungi aset dan keamanan sistem informasi.

4.3. Identifikasi Dampak Risiko

Setiap risiko yang diidentifikasi perlu dievaluasi berdasarkan dampak yang mungkin terjadi jika risiko tersebut tidak dikelola dengan baik. Dampak risiko dikelompokkan menjadi kategori seperti gangguan operasional, kerusakan fisik, hilangnya data, atau kerugian finansial. Dampak ini menunjukkan seberapa besar risiko tersebut mempengaruhi keberlangsungan bisnis organisasi. Dampak yang teridentifikasi termasuk:

Tabel 3. Tabel Identifikasi Dampak Resiko

ID	Kemungkinan Risiko	Dampak
R01	Debu	Kerusakan perangkat keras, penurunan kinerja sistem, dan biaya perawatan meningkat.
R02	Kebakaran	Kehilangan data, kerusakan infrastruktur, dan gangguan operasional yang signifikan.
R03	Banjir	Kerusakan fisik pada perangkat, kehilangan data, dan biaya pemulihan yang tinggi.
R04	Pencurian data seperti hacking	Kebocoran data sensitif, kerugian reputasi, dan potensi tindakan hukum.
R05	Human error	Kehilangan data, kesalahan dalam pengambilan keputusan, dan biaya perbaikan.
R06	Penyalahgunaan hak akses	Kerusakan data, pencurian informasi, dan potensi tindakan hukum.
R07	Kerusakan perangkat keras	Downtime sistem, biaya penggantian, dan gangguan operasional.
R08	Serangan virus	Kerusakan data, gangguan sistem, dan biaya pemulihan yang tinggi.
R09	Data hilang	Kehilangan informasi penting, gangguan operasional, dan biaya pemulihan.

Tabel identifikasi dampak risiko menunjukkan berbagai risiko yang dihadapi PT XYZ dan dampak yang mungkin terjadi. Setiap risiko, seperti kebakaran atau pencurian data, dapat menyebabkan kerugian finansial, kerusakan infrastruktur, dan hilangnya kepercayaan pelanggan. Dengan memahami dampak ini, PT XYZ dapat merencanakan langkah mitigasi yang lebih baik untuk melindungi aset dan operasional perusahaan.

4.4. Analisis Risiko

Analisis risiko adalah langkah penting setelah Identifikasi Risiko. Pada tahap ini, setiap risiko yang telah diidentifikasi akan dianalisis untuk memahami seberapa besar dampak dan kemungkinan terjadinya risiko tersebut terhadap aset teknologi informasi organisasi. Tujuan dari analisis risiko adalah untuk memberikan penilaian kuantitatif atau kualitatif mengenai risiko, sehingga manajemen dapat memprioritaskan risiko-risiko yang paling signifikan dan menentukan langkah mitigasi yang tepat.

Tabel 4. Likehood

Likehood		Deskripsi	Frekuensi Kejadian
Nilai	Kriteria		
1	Rare	Risiko hampir tidak pernah terjadi.	>2 tahun
2	Unlikely	Risiko terjadi sesekali.	1-2 tahun
3	Possible	Risiko terjadi dengan frekuensi sedang.	7-12 bulan
4	Likely	Risiko sering terjadi	4-6 bulan
5	Almost Certain	Risiko hampir selalu terjadi.	1-3 bulan

Tabel likehood menunjukkan kriteria kemungkinan terjadi yang digunakan dalam evaluasi risiko untuk menentukan seberapa sering risiko tertentu kemungkinan terjadi. Setiap tingkat kemungkinan terjadi memiliki nilai dari 1 hingga 5, dengan deskripsi dan jangka waktu kejadian yang terkait.

Tabel 5. Impact

Impact		Deskripsi
Nilai	**Kriteria**	
1	Insignificant	Dampak tidak signifikan, hampir tidak ada gangguan operasional.
2	Minor	Dampak kecil, gangguan minimal yang tidak mempengaruhi operasi utama.
3	Moderate	Dampak sedang, mempengaruhi sebagian besar operasional sementara waktu.
4	Major	Dampak signifikan yang mempengaruhi sebagian besar operasional.
5	Catastrophic	Dampak serius yang menghentikan operasional atau menyebabkan kerugian besar.

Tabel impact menjelaskan kriteria dampak yang digunakan untuk menilai seberapa besar pengaruh risiko terhadap operasional organisasi. Setiap tingkat dampak memiliki nilai dari 1 hingga 5, dengan deskripsi yang sesuai.

Tabel 6. Tabel Penilaian Risiko

ID	Kemungkinan Risiko	Likehood	Impact
R01	Debu	3	2
R02	Kebakaran	1	5
R03	Banjir	2	4
R04	Pencurian data seperti hacking	3	5
R05	Human error	4	3
R06	Penyalahgunaan hak akses	3	4
R07	Kerusakan perangkat keras	3	3
R08	Serangan virus	4	4
R09	Data hilang	3	5

Tabel penilaian risiko mengidentifikasi dampak risiko di PT XYZ memberikan gambaran terstruktur mengenai berbagai risiko yang dihadapi perusahaan, termasuk frekuensi kejadian (Likelihood) dan tingkat dampak (Impact) jika risiko tersebut terjadi. Dengan menggunakan skala yang jelas, tabel ini memungkinkan manajemen untuk menilai dan memprioritaskan risiko berdasarkan total risiko yang dihitung dari perkalian likelihood dan impact.

4.5. Evaluasi Risiko

Pada tahap evaluasi risiko, setiap risiko yang telah dianalisis sebelumnya dikaji secara mendalam untuk menetapkan urutan prioritas penanganan berdasarkan tingkat signifikansi dan potensi dampaknya. Evaluasi ini bertujuan untuk menentukan apakah risiko tersebut dapat diterima, memerlukan mitigasi segera, atau hanya perlu dipantau. Pada tahap ini, risiko yang teridentifikasi akan dibandingkan dengan kriteria risiko yang telah ditentukan oleh organisasi, sehingga manajemen dapat memutuskan tindakan apa yang perlu diambil terhadap setiap risiko.

Tabel 7. Matriks Evaluasi Risiko

Impact	Likehood				
	1	**2**	**3**	**4**	**5**
1	L	L	L	M	H
2	L	L	M	M	H
3	L	M	M	M	H
4	M	M	M	H	H
5	H	H	H	H	H

Keterangan :
L : Low
M : Medium
H : Hgh

Tabel 8. Matriks Evaluasi Risiko Berdasarkan Likehood dan Impact

Impact	Likehood				
	1	**2**	**3**	**4**	**5**
1					
2			R01		
3			R07	R05	
4		R03	R06	R08	
5	R02		R04, R09		

Tabel 8 merupakan matriks evaluasi risiko berdasarkan kemungkinan terjadi dan dampak. Matriks ini digunakan untuk mengevaluasi risiko berdasarkan dua faktor utama: kemungkinan terjadi dan dampak. Risiko yang diidentifikasi dalam tabel sebelumnya telah ditempatkan pada matriks ini sesuai dengan nilai kemungkinan terjadi dan dampaknya.

Tabel 9. Tabel Tingkat Risiko

ID	Kemungkinan Risiko	Like hood	Impact	Risk Level
R02	Kebakaran	1	5	High
R04	Pencurian data seperti hacking	3	5	High
R08	Serangan virus	4	4	High
R09	Data hilang	3	5	High
R01	Debu	3	2	Medium
R03	Banjir	2	4	Medium
R05	Human error	4	3	Medium
R06	Penyalahgunaan hak akses	3	4	Medium
R07	Kerusakan perangkat keras	3	3	Medium

Tabel Tingkat risiko menunjukkan evaluasi risiko berdasarkan kemungkinan terjadi dan dampak serta level risiko. Setiap risiko telah diberi nilai berdasarkan dua faktor: kemungkinan terjadi dan dampak, yang selanjutnya menghasilkan level risiko.

4.6. Perlakuan Risiko

Perlakuan risiko merupakan tahap kritis terakhir dalam alur manajemen risiko, di mana organisasi merancang dan mengimplementasikan strategi mitigasi yang spesifik untuk risiko-risiko yang telah melalui proses identifikasi, analisis, dan evaluasi sebelumnya. Fokus utama dari tahap ini adalah meminimalisasi potensi dampak atau probabilitas kemunculan risiko, atau keduanya, sehingga risiko dapat dikelola dalam batas toleransi yang dapat diterima organisasi. Pada tahap ini, berbagai strategi

diterapkan untuk menghadapi risiko berdasarkan hasil evaluasi risiko.

Tabel 10. Tabel Penanganan Risiko

ID	Kemungkinan Risiko	Risk Level	Tindak Lanjut
R02	Kebakaran	High	Instalasi sistem pemadam kebakaran otomatis. Pelatihan karyawan tentang prosedur evakuasi.
R04	Pencurian data seperti hacking	High	Implementasi firewall dan antivirus yang kuat. Pelatihan keamanan siber untuk karyawan.
R08	Serangan virus	High	Pembaruan rutin perangkat lunak keamanan. Pemantauan sistem secara berkala.
R09	Data hilang	High	Penerapan sistem backup data secara berkala. Pengujian pemulihan data secara berkala.
R01	Debu	Medium	Pembersihan rutin area kerja. Penggunaan filter udara.
R03	Banjir	Medium	Penilaian risiko lokasi dan perencanaan mitigasi. Pembangunan saluran drainase yang baik.
R05	Human error	Medium	Pelatihan karyawan tentang prosedur kerja. Implementasi sistem verifikasi data.
R06	Penyalahgunaan hak akses	Medium	Audit akses secara berkala. Penerapan kontrol akses berbasis peran.
R07	Kerusakan perangkat keras	Medium	Pemeliharaan rutin perangkat keras. Penyediaan perangkat cadangan

Tabel 10 merupakan tabel penanganan risiko, yang menunjukkan langkah-langkah yang diambil untuk mengatasi berbagai risiko yang telah dievaluasi berdasarkan level risiko. Tabel ini memberikan panduan mengenai tindakan mitigasi yang diterapkan untuk setiap risiko guna mengurangi dampak atau kemungkinan terjadinya risiko tersebut.

5. KESIMPULAN DAN SARAN

Dalam penelitian ini, analisis manajemen risiko teknologi informasi di PT XYZ menggunakan standar ISO 31000 menunjukkan bahwa penerapan manajemen risiko yang sistematis dan komprehensif sangat penting untuk keberlangsungan organisasi di era digital. Identifikasi risiko yang mencakup faktor alam, manusia, dan sistem mengungkapkan berbagai potensi ancaman, seperti kebakaran, pencurian data, dan serangan virus, yang dapat berdampak signifikan terhadap operasional dan reputasi perusahaan. Melalui evaluasi risiko yang melibatkan penilaian likelihood dan impact, PT XYZ dapat memprioritaskan risiko-risiko yang perlu ditangani secara mendesak. Tindakan mitigasi yang diusulkan, seperti instalasi sistem pemadam kebakaran otomatis dan pelatihan keamanan siber, dirancang untuk meminimalkan eksposur risiko. Melalui penelitian ini, diharapkan dapat tercipta model pendekatan sistematis dalam mengelola risiko teknologi informasi yang dapat diadopsi oleh berbagai perusahaan, dengan menekankan pentingnya keterlibatan manajemen dalam setiap tahap proses pengelolaan risiko.

DAFTAR PUSTAKA

[1] V. R. Putri and A. F. Wijaya, "Information Technology Risk Management Analysis Using ISO: 31000 at PT. XYZ," *Journal of Information Systems and Informatics*, vol. 4, no. 3, 2022, [Online]. Available: http://journal-isi.org/index.php/isi

[2] A. Agustian Herlambang, A. A. Gani, and D. D. Alvianto, "JICN: Jurnal Intelek dan Cendikiawan Nusantara Pendekatan ISO 31000:2018 dalam Manajemen Risiko Teknologi Informasi pada Tracer Study Universitas Sebelas April ISO 31000:2018 Approach to Information Technology Risk Management in the Tracer Study at Universitas Sebelas April", [Online]. Available: https://jicnusantara.com/index.php/jicn

[3] H. B. M. Mamuaja and A. D. Cahyono, "SIOLGA Information Technology Risk Management Analysis Using ISO 31000," *Journal of Information Systems and Informatics*, vol. 6, no. 1, pp. 57–67, Mar. 2024, doi: 10.51519/journalisi.v6i1.641.

[4] S. R. Anindya, "Potential risk management design based on ISO 31000:2018 a case study of RSUD BLUD X," vol. 1, pp. 1–9, 2023, doi: 10.20885/InCAF.vol1.art1.

[5] V. Patrick, P. Wijaya, and A. D. Manuputty, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," vol. 9, no. 2, pp. 1295–1307, 2022.

[6] A. A. Putri and D. I. Irnanda, "ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 (STUDI KASUS: LAYANAN EKSPEDISI XYZ) INFORMATION TECHNOLOGY RISK ANALYSIS USING ISO 31000 (CASE STUDY: XYZ EXPEDITION SERVICE)," *Jurnal Teknologi dan Terapan Bisnis (JTTB)*, vol. 6, no. 1, p. 18, 2023.

[7] H. I. Pribadi and E. Ernastuti, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina)," *JURNAL SISTEM INFORMASI BISNIS*, vol. 10, no. 1, pp. 28–35, May 2020, doi: 10.21456/vol10iss1pp28-35.

[8] A. Aisyah Ulfa, "Analisis Manajemen Risiko Dengan Penerapan ISO 31000 Pada Proses

Machining (Studi Kasus: Perusahaan AB) Risk Management Analysis Using ISO 31000 at Machining Process (Case Study: AB Company)." [Online]. Available: http://jurnal.um-palembang.ac.id/integrasi/index

[9] E. Evinia and M. N. N. Sitokdana, "Risk Management Based IT Analysis Using ISO 31000 (Case Study: PT Bawen Mediatama)," *Journal of Information Systems and Informatics*, vol. 5, no. 1, pp. 380–390, Mar. 2023, doi: 10.51519/journalisi.v5i1.420.

[10] G. Gerald Moleong and A. Rocky Tanaamah, "ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA APLIKASI INLISLITE DI DINAS KEARSIPAN DAN PERPUSTAKAAN PROVINSI NUSA TENGGARA TIMUR," 2022.

[11] B. Prasetyo, A. Salsabila, and W. E. Y. Retnani, "Prasetyo, Salsabila, Retnani (IT Risk Management Analysis Based on ISO 31000 and Bow Tie Analysis (BTA) in Higher Education Institution)," 2024.

[12] R. D. B. Bachtiar and Machmudin Eka Prasetya, "Evaluation of Risk Management Implementation in IT Projects Using ISO 31000 in an ICT Solutions Company," *Accounting and Finance Studies*, vol. 4, no. 1, pp. 17–33, Jan. 2024, doi: 10.47153/afs41.8682024.

[13] N. L. Putri and A. F. Wijaya, "Information Technology Risk Management in Educational Institutions Using ISO 31000 Framework," *Journal of Information Systems and Informatics*, vol. 5, no. 2, pp. 630–649, May 2023, doi: 10.51519/journalisi.v5i2.468.

[14] M. I. Fachrezi, A. Dwika Cahyono, and P. F. Tanaem, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga," *Jurusan Sistem Informasi*, vol. 8, no. 2, 2021, [Online]. Available: http://jurnal.mdp.ac.id

[15] S. A. Atmojo and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office," 2020. [Online]. Available: http://jurnal.mdp.ac.id

[16] F. Wati, S. Sari, and J. N. Utamajaya, "IT Risk Management based on ISO 31000 For BRImo Application (BRI Mobile) as an Transaction Processing Information System," 2021.