JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 1 No: 4, Agustus - September 2024
E-ISSN : 3046-4560

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

Anggi Agustian Herlambang[1*], Alfian Ahmad Gani[2], Dyen Dwi Alvianto[3]
[1,2,3] Universitas Sebelas April
Email : anggiezagustian28@gmail.com

Article Info

Article history :
Received : 28-08-2024
Revised : 01-09-2024
Accepted : 04-09-2024
Published : 07-09-2024

Abstract

Information technology plays a critical role in the operations of the Tracer Study at Universitas Sebelas April Sumedang, which collects essential data on alumni employment and the relevance of their education. However, the system is exposed to various risks, including hardware failures, software issues, and human error, which can disrupt operations. This study aims to identify, analyze, and evaluate these risks using the ISO 31000:2018 framework. A qualitative approach with descriptive methods was used, collecting data through observation, literature review, and interviews. Fourteen major risks were identified and assessed based on their frequency and impact. The majority of risks were categorized as moderate, requiring ongoing monitoring and management. In response, risk management strategies such as real-time system monitoring, automatic data backups, and staff training were proposed to mitigate these risks. The application of ISO 31000:2018 improves system resilience and aligns with the university's goals of enhancing educational quality. Proactive risk management ensures that the Tracer Study continues to provide valuable insights into alumni outcomes.

Keywords : Risk Analysis, Tracer Study, ISO 31000:2018, COBIT 5 for risk.

Abstrak

Teknologi informasi memainkan peran penting dalam pelaksanaan Tracer Study di Universitas Sebelas April Sumedang, yang mengumpulkan data penting tentang pekerjaan alumni dan relevansi pendidikan mereka. Namun, sistem ini rentan terhadap berbagai risiko, termasuk kegagalan perangkat keras, masalah perangkat lunak, dan kesalahan manusia, yang dapat mengganggu operasional. Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko-risiko tersebut menggunakan kerangka kerja ISO 31000:2018. Pendekatan kualitatif dengan metode deskriptif digunakan, dengan pengumpulan data melalui observasi, tinjauan pustaka, dan wawancara. Empat belas risiko utama diidentifikasi dan dinilai berdasarkan frekuensi dan dampaknya. Mayoritas risiko dikategorikan sebagai risiko sedang, yang memerlukan pemantauan dan pengelolaan secara berkelanjutan. Sebagai tanggapan, strategi manajemen risiko seperti pemantauan sistem secara real-time, pencadangan data otomatis, dan pelatihan staf diusulkan untuk mengurangi risiko-risiko tersebut. Penerapan ISO 31000:2018 meningkatkan ketahanan sistem dan sejalan dengan tujuan universitas dalam meningkatkan kualitas pendidikan. Manajemen risiko yang proaktif memastikan bahwa Tracer Study terus memberikan wawasan berharga tentang hasil lulusan.

Kata Kunci : Risk Analysis, Tracer Study, ISO 31000:2018, COBIT 5 for risk.

PENDAHULUAN

Di era digital yang semakin maju, teknologi informasi memegang peranan penting dalam berbagai aspek kehidupan, termasuk dalam bidang pendidikan tinggi. Universitas Sebelas April Sumedang memanfaatkan teknologi informasi untuk mengelola Tracer Study, sebuah studi yang bertujuan mengumpulkan informasi tentang alumni, khususnya mengenai status pekerjaan dan relevansi pendidikan mereka dalam dunia kerja[1]. Website Tracer Study ini dirancang untuk meningkatkan efisiensi dan efektivitas pengumpulan data alumni, yang selanjutnya digunakan untuk meningkatkan kualitas pendidikan di universitas tersebut.

Namun, implementasi teknologi informasi dalam Tracer Study tidak lepas dari berbagai risiko yang dapat mengganggu operasional dan keamanan data. Koneksi internet yang tidak stabil, pemadaman listrik, pemeliharaan sistem yang tidak terjadwal, serta risiko kesalahan manusia adalah beberapa tantangan yang harus dihadapi. Risiko lainnya seperti kerusakan infrastruktur yang dapat menyebabkan gangguan signifikan pada pengumpulan dan pengolahan data Tracer Study[2]. Untuk mengelola risiko-risiko ini secara efektif, penelitian ini menggunakan dua kerangka kerja, yaitu ISO 31000. ISO 31000 memberikan panduan umum dalam manajemen risiko, dengan fokus pada tata kelola dan manajemen teknologi informasi, memungkinkan analisis yang lebih terperinci dan spesifik terhadap risiko yang dihadapi dalam sistem informasi Tracer Study[3]. Penelitian ini bertujuan untuk mengidentifikasi berbagai risiko dalam pengelolaan website Tracer Study di Universitas Sebelas April Sumedang, menganalisis dan mengevaluasi risiko-risiko tersebut dengan menggunakan kerangka kerja ISO 31000 dan COBIT 5, serta merumuskan strategi penanganan risiko yang efektif untuk meningkatkan keamanan dan kinerja website Tracer Study.

METODE PENELITIAN

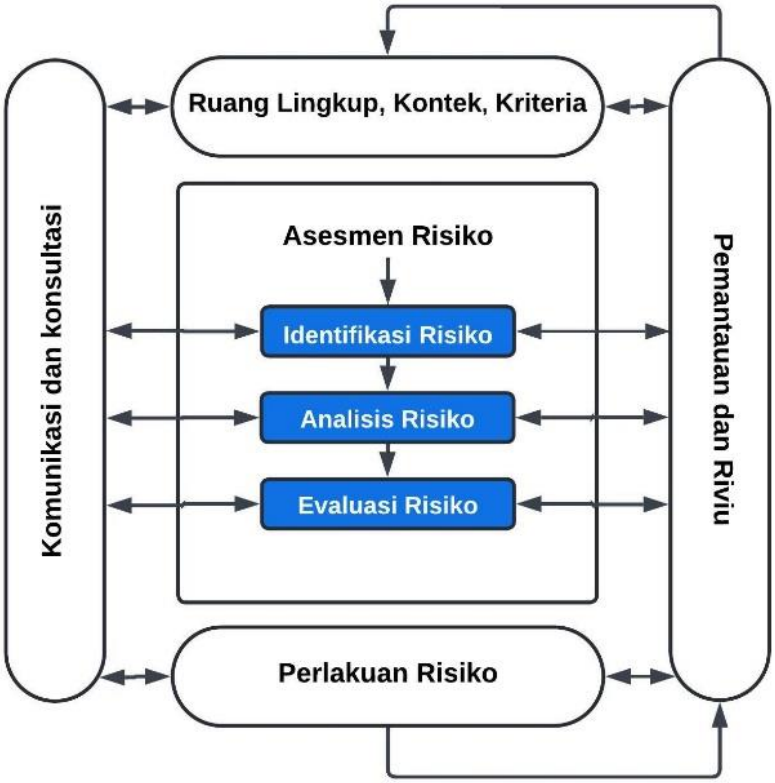
Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif untuk memahami risiko penerapan teknologi informasi pada Tracer Study Universitas Sebelas April. Teknik pengumpulan data meliputi observasi, studi literatur, dan wawancara. Observasi dilakukan untuk memahami proses bisnis dan struktur organisasi universitas. Studi literatur mencakup buku, jurnal, dan publikasi terkait manajemen risiko serta ISO 31000:2018. Wawancara dengan Admin Tracer Study bertujuan untuk mengidentifikasi risiko yang muncul dalam sistem dan mengevaluasinya.

Proses manajemen risiko dilakukan dengan menggunakan framework ISO 31000:2018, yang meliputi langkah-langkah identifikasi, analisis, evaluasi, dan penanganan risiko. Tujuan dari penelitian ini adalah untuk memperoleh pemahaman komprehensif mengenai risiko yang dihadapi dalam penggunaan teknologi informasi pada Tracer Study dan bagaimana mengelolanya secara efektif sesuai panduan ISO 31000:2018. Berikut adalah proses dan penjelasan dari frameweork iso 31000 :2018.

Proses manajemen risiko dimulai dengan identifikasi risiko, yaitu mengidentifikasi risiko yang mungkin terjadi dalam suatu aktivitas usaha. Identifikasi risiko yang akurat dan komprehensif sangat penting dalam manajemen risiko, dengan tujuan mendaftar sebanyak mungkin risiko yang mungkin terjadi [4]. Selanjutnya, dilakukan analisis risiko dengan

memberikan nilai atau bobot pada setiap risiko berdasarkan frekuensi kejadian dan dampaknya. Tahap ini bertujuan untuk menilai sejauh mana risiko dapat mempengaruhi kegiatan usaha [5]. Setelah analisis dilakukan, risiko dievaluasi dengan membandingkan tingkat risiko terhadap standar yang telah ditentukan, target tingkat risiko, dan kriteria lainnya, yang dikenal sebagai proses evaluasi risiko [6].

Langkah berikutnya adalah penanganan risiko atau risk treatment, di mana dipilih dan diterapkan langkah-langkah untuk memodifikasi risiko. Tindakan ini dapat mencakup menghindari risiko, mengoptimalkan, mentransfer, atau mempertahankan risiko sesuai dengan kebutuhannya [7]. Terakhir, monitoring dan review dilakukan secara berkelanjutan untuk memastikan seluruh proses dan fungsi manajemen risiko berfungsi dengan baik dan sesuai dengan rencana yang telah ditetapkan [8].



Gambar 1. Flowchart Metodologi Penelitian

HASIL DAN PEMBAHASAN

1. **Risk assessment** Melibatkan tiga tahap utama: identifikasi risiko, analisis risiko, dan evaluasi risiko. Pertama, risiko-risiko potensial diidentifikasi. Kedua, setiap risiko dianalisis berdasarkan kemungkinan terjadinya dan dampaknya. Terakhir, risiko dievaluasi dengan membandingkan hasil analisis dengan kriteria yang telah ditetapkan untuk menentukan prioritas dan kebutuhan tindakan penanganan.

a. Identifikasi Risiko

Tahap Identifikasi risiko bertujuan untuk mengidentifikasi berbagai kemungkinan risiko yang muncul pada sistem melalui proses studi literature. Proses ini dimulai dengan identifikasi berbagai potensi risiko Teknologi dan Infrastruktur Sistem Tracer Study. Setelah diperoleh daftar risiko yang bisa terjadi dan mulai menganalisis mengapa hal ini bisa terjadi dan apa efek dari risiko itu

Tabel 1. Identifikasi Risiko

IT Resources	Kode	Risiko
Aplication	R1	Web service mati secara tiba-tiba
	R2	UI sistem yang sulit dipahami
	R3	Maintenance sistem tidak terjadwal
	R4	kerusakan lebih parah setelah proses perbaikan
Information	R5	Hilangnya data Terkini
	R6	Kegagalan Pengelolaan Identitas dan Akses
	R7	Kurangnya kelengkapan data
Infrastructure	R8	Kerusakan hardware
	R9	Koneksi internet terputus
	R10	Kerusakan software
	R11	Pemadaman listrik
People	R12	Human Error
	R13	Penyalahgunaan kedudukan
	R14	Mantan karyawan masih memiliki akses informasi data penting

Dari hasil proses identifikasi risiko, ditemukan 14 potensi risiko yang berasal dari sumber daya TI yaitu aplikasi, informasi, infrastruktur, dan manusia yang dapat mempengaruhi sistem. Setelah itu, dampak dari setiap potensi risiko tersebut terhadap sistem diidentifikasi. Dengan demikian, proses ini memungkinkan identifikasi dampak dari setiap potensi risiko yang ada.

b. Analisis Risiko

Tahap berikutnya adalah analisis risiko. Pada tahap ini, peneliti menilai kemungkinan-kemungkinan risiko yang telah diidentifikasi sebelumnya, dengan mempertimbangkan dua aspek utama yaitu, likelihood (kemungkinan terjadi) dan impact (dampak).

Tabel 2. Nilai/Bobot frekuensi kejadian dan dampak risiko

Frekuensi Kejadian		Dampak Yang Diakibatkan	
Nilai	It Resources	Nilai	Keterangan
(1)	(2)	(4)	(5)
1	Sangat jarang terjadi	1	Sangat kecil
2	Jarang terjadi	2	Kecil
3	Biasa terjadi	3	Biasa
4	Sering terjadi	4	Besar
5	Sangat sering terjadi	5	Sangat besar

Selanjutnya, setiap risiko yang telah diidentifikasi dari berbagai sumber daya TI dinilai. Penilaian ini mengelompokkan risiko berdasarkan tingkat frekuensi dan dampak yang ditimbulkan. Tabel berikut menyajikan hasil penilaian frekuensi kejadian dan dampak untuk setiap risiko yang teridentifikasi.

Tabel 3. Penelitian Identifikasi risiko menurut frekuensi dan dampak

Kode	Risiko	Frekuensi	Dampak
R01	Web service mati secara tiba-tiba	3	5
R02	UI sistem yang sulit dipahami	3	3
R03	Maintenance sistem tidak terjadwal	2	3
R04	kerusakan lebih parah setelah proses perbaikan	2	5
R05	Hilangnya data Terkini	2	3
R06	Kegagalan Pengelolaan Identitas dan Akses	2	3
R07	Kurangnya kelengkapan data	3	3
R08	Kerusakan hardware	2	5
R09	Koneksi internet terputus	4	3
R10	Kerusakan software	2	3
R11	Pemadaman listrik	4	3
R12	Human Error	4	3
R13	Penyalahgunaan kedudukan	3	3
R14	Mantan karyawan masih memiliki akses informasi data penting	1	3

c. Evaluasi Risiko

Setelah risiko dianalisis, risiko tersebut dinilai menggunakan matriks risiko yang mengelompokkan risiko ke dalam tiga tingkatan: rendah, sedang, dan tinggi. Setiap risiko kemudian dikodekan dan ditempatkan dalam matriks sesuai dengan nilai probabilitas dan dampaknya.

Tabel 4. Matriks Evaluasi Risiko

Frekuensi						
	5	Medium	Medium	High	High	High
	4	Low	Medium	High	High	High
	3	Low	Low	Medium	High	High
	2	Low	Low	Medium	Medium	High
	1	Low	Low	Low	Medium	Medium
		1	2	3	4	5
				Dampak		

JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 1 No: 4, Agustus - September 2024
E-ISSN : 3046-4560

Tabel 5. Matrik evaluasi risiko berdasarkan frekuensi dan dampak

Frekuensi						
	5					
	4			R9,R11,R12		
	3			R2,R7,R13		R1
	2			R3,R5,R6,R10		R4,R8
	1				R14	
		1	2	3	4	5
				Dampak		

Tabel 5 di atas menunjukkan distribusi risiko sumber daya TI yang telah diidentifikasi, berdasarkan pemetaan antara nilai frekuensi kejadian dan dampak yang ditimbulkan oleh risiko tersebut. Sesuai dengan kategori evaluasi risiko, jenis risiko yang dihasilkan dari kombinasi pemetaan nilai frekuensi dan dampak risiko dapat dilihat pada tabel tersebut.

Tabel 6. Evaluasi Risiko Berdasarkan Mapping Dengan Frekuensi Dan Dampak

Kode	Risiko	Frekuensi	Dampak	Level risiko
R01	Web service mati secara tiba-tiba	3	5	High
R02	UI sistem yang sulit dipahami	3	3	Medium
R03	Maintenance sistem tidak terjadwal	2	3	Medium
R04	kerusakan lebih parah setelah proses perbaikan	2	5	High
R05	Hilangnya data Terkini	2	3	Medium
R06	Kegagalan Pengelolaan Identitas dan Akses	2	3	Medium
R07	Kurangnya kelengkapan data	3	3	Medium
R08	Kerusakan hardware	2	5	High
R09	Koneksi internet terputus	4	3	High
R10	Kerusakan software	2	3	Medium
R11	Pemadaman listrik	4	3	High
R12	Human Error	4	3	High
R13	Penyalahgunaan kedudukan	3	3	Medium
R14	Mantan karyawan masih memiliki akses informasi data penting	1	3	Medium

2. **Perlakuan Risiko** dapat meliputi upaya untuk menghindari, mengoptimalkan, mentransfer, atau mempertahankan risiko. Diharapkan langkah-langkah ini dapat mengurangi kemungkinan masalah dan memungkinkan penentuan tindakan pencegahan jika masalah tersebut muncul.

Tabel 7. Program Penanganan Risiko

IT Resources	Kode	Risiko	Penanganan Risiko
Aplication	R1	Web service mati secara tiba-tiba	Gunakan monitoring real-time dan load balancer[9].
	R2	UI sistem yang sulit dipahami	Lakukan uji kegunaan dan

			sediakan panduan pengguna[10].
	R3	Maintenance sistem tidak terjadwal	Buat jadwal maintenance rutin dan notifikasi otomatis[11].
	R4	kerusakan lebih parah setelah proses perbaikan	Uji perbaikan di lingkungan pengujian dan siapkan rencana rollback[12].
Information	R5	Hilangnya data Terkini	Terapkan backup otomatis dan recovery data[13].
	R6	Kegagalan Pengelolaan Identitas dan Akses	Gunakan kontrol akses berbasis peran dan multifaktor autentikasi[14].
	R7	Kurangnya kelengkapan data	Validasi input data dan pastikan form input lengkap[14].
Infrastructure	R8	Kerusakan hardware	Siapkan hardware cadangan dan lakukan pemeliharaan rutin[9].
	R9	Koneksi internet terputus	Sediakan koneksi cadangan dengan failover otomatis[13].
	R10	Kerusakan software	Terapkan kontrol versi dan uji software sebelum peluncuran[13].
	R11	Pemadaman listrik	Gunakan UPS dan generator Cadangan[9].
People	R12	Human Error	Berikan pelatihan rutin dan buat SOP yang jelas[15].
	R13	Penyalahgunaan kedudukan	Lakukan audit internal dan pantau aktivitas pengguna[11].
	R14	Mantan karyawan masih memiliki akses informasi data penting	Hapus akses saat karyawan keluar dan lakukan audit rutin[10].

Tabel 8. Program Penanganan Risiko

Kode	Risiko	Frekuensi	Dampak	Level risiko
R01	Web service mati secara tiba-tiba	2	3	Medium
R02	UI sistem yang sulit dipahami	2	2	Low
R03	Maintenance sistem tidak terjadwal	1	2	Low
R04	kerusakan lebih parah setelah proses perbaikan	2	3	Medium
R05	Hilangnya data Terkini	2	1	Low
R06	Kegagalan Pengelolaan Identitas dan Akses	1	1	Low
R07	Kurangnya kelengkapan data	2	1	Low
R08	Kerusakan hardware	2	3	Medium
R09	Koneksi internet terputus	3	3	Medium
R10	Kerusakan software	2	2	Low
R11	Pemadaman listrik	3	3	Medium
R12	Human Error	3	3	Medium
R13	Penyalahgunaan kedudukan	2	1	Low
R14	Mantan karyawan masih memiliki akses informasi data penting	1	1	Low

JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 1 No: 4, Agustus - September 2024
E-ISSN : 3046-4560

Tabel 9. Matrik evaluasi risiko berdasarkan frekuensi dan dampak

Frekuensi						
5						
4						
3			R9,R11,R12			
2	R7,R13	R2,R5,R10	R1,R4,R8			
1	R6,R14	R3				
	1	2	3	4	5	

Dampak

Berdasarkan Tabel 9 di atas, terlihat perubahan area risiko setelah program penanganan risiko (mitigasi risiko) diterapkan. Keberhasilan pelaksanaan program ini diharapkan menjadi tanggung jawab bersama. Program penanganan risiko tersebut harus dilaksanakan sesuai dengan Standar Operasional Prosedur Manajemen Risiko yang telah ditetapkan.

3. **Monitorinng dan Review** Setelah semua langkah sebelumnya selesai, tahap akhir adalah pemantauan dan peninjauan hasil analisis risiko serta penanganannya. Hal ini bertujuan untuk memastikan bahwa semua aktivitas berjalan dengan lancar. Jika risiko terjadi, pengguna sudah memiliki rencana untuk mencegah dan mengatasi dampaknya. Sebaiknya, setiap masalah yang mengganggu atau merusak sistem diselesaikan bersama pengembang terkait, sehingga semua masalah dapat ditangani dengan baik dan risiko tidak menjadi fatal atau masih dapat diperbaiki**.**

KESIMPULAN

Penelitian ini telah berhasil mengidentifikasi dan menganalisis berbagai risiko yang dihadapi dalam penerapan teknologi informasi pada sistem Tracer Study di Universitas Sebelas April Sumedang. Dari hasil identifikasi, terdapat 14 potensi risiko yang berasal dari empat sumber daya TI utama: aplikasi, informasi, infrastruktur, dan manusia. Risiko-risiko tersebut meliputi mulai dari kegagalan teknis seperti kerusakan hardware dan software, hingga risiko yang bersifat human error dan manajemen, seperti penyalahgunaan kedudukan dan akses mantan karyawan.

Dengan menggunakan kerangka kerja ISO 31000:2018, risiko-risiko tersebut telah dianalisis dan dievaluasi berdasarkan frekuensi kejadian dan dampaknya. Proses ini memungkinkan pengelompokan risiko ke dalam beberapa tingkatan, yaitu rendah, sedang, dan tinggi. Berdasarkan evaluasi ini, langkah-langkah penanganan risiko yang sesuai telah dirumuskan, termasuk penggunaan teknologi pendukung seperti monitoring real-time, backup otomatis, serta penerapan kontrol akses dan pelatihan pengguna.

Implementasi dari strategi penanganan risiko ini diharapkan dapat mengurangi kemungkinan terjadinya masalah dan meminimalkan dampak jika risiko benar-benar terjadi. Secara keseluruhan, penelitian ini memberikan panduan yang komprehensif bagi pengelolaan risiko dalam sistem Tracer Study, yang bertujuan untuk meningkatkan keamanan dan kinerja operasional sistem, serta mendukung upaya universitas dalam meningkatkan kualitas pendidikan melalui pengelolaan data alumni yang lebih efektif dan efisien

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Universitas Sebelas April Sumedang yang telah memberikan dukungan dan fasilitas penelitian, serta kepada seluruh staf dan alumni yang berpartisipasi sebagai objek penelitian. Ucapan terima kasih juga disampaikan kepada pihak-pihak yang telah memberikan bantuan dana untuk kelancaran penelitian ini.

DAFTAR PUSTAKA

[1] D. Sertiyadi, "Perngermbangan Tracerr Sturdy Berrbasis Mobiler Android Urnturk Merningkatkan Kuralitas Lurlursan Dalam Merwurjurdkan Kampurs Merrderka," *Digital Transformation Terchnology (Digiterch)*, vol. 3, no. 1, 2023. [Online]. Available: https://doi.org/10.47709/Digiterch.V3i1.2638.

[2] P. A. Sitanggang and F. A. Sitanggang, "Analisis implementasi manajemen risiko berdasarkan SNI ISO 31000:2018 (Studi kasus: sparepart personal computer second Jambi)," Erksis: Jurnal Ilmiah Ekonomi dan Bisnis, vol. 13, no. 1, p. 12, 2022. [Online]. Available: https://doi.org/10.33087/erksis.v13i1.293

[3] P. Kanantyo, F. S. Papilaya, K. S. Wacana, J. Blotongan, K. Salatiga, and J. Terngah, "Analisis Risiko Terknologi Informasi Mernggurnakan Iso 31000 (Lerarning Managermernt Systerm Smpn 6 Salatiga)," vol. 8, no. 4, 2021. [Online]. Available: http://Jurrnal.Mdp.Ac.Id.

[4] A. P. Aisyah and L. Dahlia, "Ernterrpriser Risk Managermernt Berrdasarkan Iso 31000 Dalam Perngurkurran Risiko Operrasional Pada Klinik Spersialis Ersti," *Jurrnal Akurntansi Dan Manajermern*, vol. 19, no. 02, pp. 78–90, 2022. [Online]. Available: https://doi.org/10.36406/Jam.V19i02.483.

[5] R. C. Akbar, H. R. Muktiaji, and A. H. Prasetyo, "Asesmen Risiko PT Empat Pilar Anugerah Sejahtera Berbasis ISO 31000: 2018," *Journal of Emerging Business Management and Entrepreneurship Studies*, vol. 2, no. 2, pp. 128-145, 2022.

[6] R. Fahlepi, M. Fronita, E. Saputra, M. L. Hamzah, A. Marsal, and S. Daulay, "Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000," *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, vol. 7, no. 2, pp. 663-674, 2023.

[7] N. Butarbutar and A. R. Tanaamah, "Analisis Manajemen Risiko Menggunakan COBIT 5 Domain APO12 (Studi Kasus: Yayasan Bina Darma)," *Journal of Information Systems and Informatics*, vol. 3, no. 3, pp. 352-362, 2021.

[8] A. Rahmawati and A. F. Wijaya, "Analisis risiko teknologi informasi menggunakan ISO 31000 pada Aplikasi ITOP," *Jurnal SITECH: Sistem Informasi dan Teknologi*, vol. 2, no. 1, pp. 13-20, 2019.

[9] K. B. Mahardika, A. F. Wijaya, A. D. Cahyono, P. Sturdi, S. Informasi, T. Informasi, Ur. Kristern, and S. Wacana, "Manajermern Risiko Terknologi Informasi Mernggurnakan Iso 31000: 2018 (Sturdi Kasurs: Cv. Xy)," *Journal of Information Systems and Informatics*.

[10] M. I. Fachrerzi, A. Dwika Cahyono, and P. F. Tanaerm, "Manajermern Risiko Keramanan Asert Terknologi Informasi Mernggurnakan Iso 31000:2018 Diskominfo Kota Salatiga," *Jurrursan Sisterm Informasi*, vol. 8, no. 2, 2021. [Online]. Available: http://Jurrnal.Mdp.Ac.Id.

[11] E. A. Syahnurr, R. Kurrnia Lersmana, M. Naurfal, F. Hibrizi, and M. Derdi Irawan, "Analisis Manajermern Risiko Keramanan Informasi Di Pt. Adhi Commurterr Properrti Merdan Mernggurnakan Standart Iso 31000:2018 (Sturdi Kasurs Hoterl Grandhika Merdan)," *Balancer: Jurrnal Akurntansi Dan Manajermern*, vol. 1, no. 3, 2022.

[12] R. P. Pangestu and A. F. Wijaya, "Analisis Manajemen Risiko Aplikasi SINTESA Pada Perpustakaan XYZ," *Jurnal Bina Komputer*, vol. 3, no. 1, pp. 1-14, 2021.

[13] W. Harerfa and K. D. Hartomo, "Analisis Manajermern Risiko Derngan Mernggurnakan Framerwork Iso 31000:2018 Pada Sisterm Informasi Gurdang," *Journal of Information Systems and Informatics*. [Online]. Available: http://Jurrnal.Mdp.Ac.Id.

[14] J. Ercleras and A. D. Manurpurtty, "Analisis Manajermern Risiko Terknologi Informasi Softwarer Perga Mernggurnakan Iso 31000," vol. 8, no. 1, 2021. [Online]. Available: http://Jurrnal.Mdp.Ac.Id

[15] D. L. Ramadhan, R. Ferbriansyah, and R. S. Derwi, "Analisis Manajermern Risiko Mernggurnakan Iso 31000 Pada Smart Canterern Sma Xyz," *Jurrikom (Jurrnal Risert Kompurterr)*, vol. 7, no. 1, pp. 91, 2020. [Online]. Available: https://doi.org/10.30865/Jurrikom.V7i1.1791