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

PENERAPAN ISO 31000:2018 PADA SISTEM PENERIMAANMAHASISWA BARU UNIVERSITAS SEBELAS APRIL SUMEDANG

IMPLEMENTATION OF ISO 31000:2018 ON THE NEW STUDENT ADMISSION SYSTEM AT UNIVERSITAS SEBELAS APRIL SUMEDANG

Alfian Ahmad Gani [1*], Anggi Agustian Herlambang[2], Dyen Dwi Alvianto[3]
[1,2,3] Universitas Sebelas April Sumedang
Email : alfianahmadgani596@gmail.com

Article Info

Article history :
Received : 26-08-2024
Revised : 31-08-2024
Accepted : 02-09-2024
Published : 05-09-2024

Abstract

In today's society, life heavily depends on technology, where organizations and educational institutions significantly benefit from information systems. However, the use of this technology also carries risks that can endanger organizations both internally and externally. Universitas Sebelas April Sumedang (Unsap) is committed to becoming a leading higher education institution in information technology by building systems that support educational and service activities, one of which is the New Student Admission Information System (PENMABA). This system helps manage new student data but also presents risks related to information security and data entry errors. To manage these risks, Unsap uses the ISO 31000: 2018 risk management standard. This research employs a qualitative method with the ISO 31000 framework to identify, analyze, and evaluate the risks faced by PENMABA. The research results identified 13 risk threats consisting of 5 high risks and 8 medium risks. Based on the evaluation results, recommendations for risk management were provided to mitigate and prevent future threats. Proper risk management implementation will ensure that the information system is continuously updated and improved, supporting the goals and success of Universitas Sebelas April Sumedang..

Keywords* : *ISO 31000:2018, Risk Management, PENMABA

Abstrak

Kehidupan bermasyarakat saat ini sangat bergantung pada teknologi, di mana organisasi dan perguruan tinggi mendapat manfaat signifikan dari sistem informasi. Namun, penggunaan teknologi ini juga memiliki risiko yang dapat membahayakan organisasi, baik secara internal maupun eksternal. Universitas Sebelas April Sumedang (Unsap) berkomitmen untuk menjadi perguruan tinggi unggul dalam teknologi informasi dengan membangun sistem pendukung kegiatan pendidikan dan pelayanan, salah satunya adalah Sistem Informasi Penerimaan Mahasiswa Baru (PENMABA). Sistem ini membantu dalam mengelola data mahasiswa baru namun juga menghadirkan risiko terkait keamanan informasi dan kesalahan pengimputan data. Untuk mengelola risiko ini, Unsap menggunakan standar manajemen risiko ISO 31000: 2018. Penelitian ini menggunakan metode kualitatif dengan framework ISO 31000 untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko yang dihadapi oleh PENMABA. Hasil penelitian menemukan 13 ancaman risiko yang terdiri dari 5 risiko tinggi dan 8 risiko medium. Berdasarkan hasil evaluasi, diberikan rekomendasi penanganan risiko untuk mengurangi dan mencegah ancaman yang akan datang. Implementasi

manajemen risiko yang sesuai akan memastikan bahwa sistem informasi terus diperbarui dan ditingkatkan, mendukung tujuan dan keberhasilan Universitas Sebelas April Sumedang.

Kata Kunci : ***ISO 31000:2018, Manajemen Risiko, PENMABA***

PENDAHULUAN

Kehidupan bermasyarakat sekarang bergantung pada teknologi. Baik organisasi maupun perguruan tinggi mendapat manfaat dari teknologi sistem informasi. Namun, teknologi tidak bebas dari potensi bahaya yang dapat membahayakan organisasi secara internal maupun eksternal [1]. Upaya pengukuran risiko teknologi informasi adalah salah satu langkah awal untuk mengatasi risiko tersebut [2]. Untuk mengelola risiko dengan benar, dapat menggunakan standar manajemen risiko. ISO 31000: 2018 adalah standar manajemen risiko yang umum digunakan oleh banyak organisasi dan membantu menyederhanakan banyak hal [3]. Standar ini digunakan oleh organisasi untuk menciptakan dan melindungi aset perusahaan dengan mengelola risiko dan mendukung peningkatan kinerja perusahaan dalam semua rencana dan keputusan yang dibuat untuk mendukung keberhasilan dan tujuan perusahaan.

Universitas Sebelas April Sumedang berusaha menjadi perguruan tinggi yang unggul dalam tren teknologi informasi. Unsap berkomitmen untuk memberikan pelayanan terbaik kepada calon mahasiswa, salah satunya dengan membangun sistem yang mendukung kegiatan pendidikan dan pelayanan. Universitas Sebelas April memiliki beberapa sistem informasi. Salah satunya adalah Sistem Informasi Penerimaan Mahasiswa Baru (PENMABA), yang digunakan secara teratur oleh perguruan tinggi saat mahasiswa baru memulai kuliah. PENMABA digunakan untuk mengelola data mahasiswa baru. Hadirnya PENMABA sejak tahun 2022 dianggap sangat membantu dosen, karyawan, dan siswa dalam melaksanakan kegiatan mereka [4]. PENMABA tidak hanya bermanfaat bagi penggunanya, tetapi juga merupakan ancaman dan dapat merugikan mereka. Sistem ini memiliki kapasitas yang cukup untuk menyimpan jumlah data pribadi yang signifikan dari mahasiswa baru dan yang sudah terdaftar. Karena sistem menyimpan informasi sensitif, semua risiko harus dipertimbangkan. Selain masalah keamanan yang telah disebutkan sebelumnya, manajemen risiko PENMABA juga melibatkan kesalahan pengimputan data, yang terjadi setiap tahun saat penerimaan siswa baru. Kesalahan pengimputan data dapat menyebabkan informasi tidak akurat, dan gangguan jaringan internet dapat menyulitkan akses dan pengelolaan data siswa baru. Universitas dapat meningkatkan keandalan dan kualitas layanan sistem informasi PENMABA dengan mengidentifikasi dan mengelola ancaman ini.

Tujuan dari implementasi manajemen risiko ini adalah untuk mengurangi semua risiko yang sedang terjadi dan yang mungkin terjadi di kemudian hari. Manajemen risiko juga akan memberikan rekomendasi yang sesuai untuk Sistem Informasi Penerimaan Mahasiswa Baru Universitas Sebelas April mengenai potensi risiko. ISO 31000: 2018 menyediakan kerangka kerja untuk pengawasan dan evaluasi terus-menerus keberhasilan strategi manajemen risiko. Hal ini penting untuk memastikan bahwa sistem informasi terus diperbarui dan ditingkatkan untuk mengantisipasi perubahan lingkungan risiko [5].

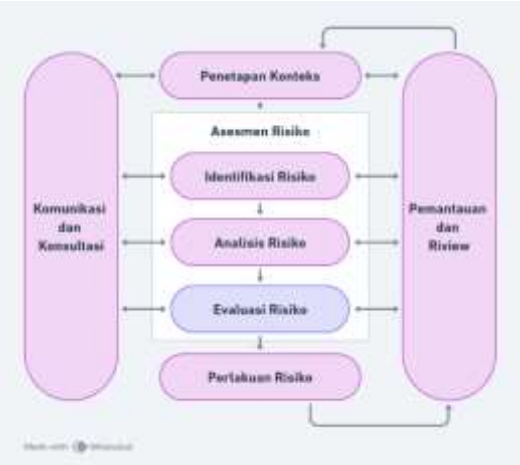
JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 1 No: 4, Agustus - September 2024
E-ISSN : 3046-4560

METODE PENELITIAN

Peneliti menggunakan metode penelitian kualitatif. Penelitian kualitatif adalah jenis penelitian yang bertujuan untuk mengidentifikasi, menemukan, menggambarkan, dan menjelaskan kualitas atau keunggulan dari pengaruh sosial yang tidak dapat dijelaskan, diukur, atau digambarkan melalui pendekatan kuantitatif pada studi kasus alamiah dengan menggunakan berbagai metode alamiah. Penelitian kasus adalah metode yang digunakan dalam penelitian ini karena hanya berfokus pada satu subjek studi kasus. Tujuan dari metode studi kasus ini adalah untuk memberi peneliti kesempatan untuk berkonsentrasi lebih lanjut pada subjek penelitian mereka setelah mereka mengumpulkan data yang diperlukan.

Peneliti menggunakan framework ISO 31000 untuk mengelola manajemen risiko di Universitas Sebelas April ini. ISO 31000 berfokus pada manajemen risiko dan telah berkembang menjadi standar manajemen risiko di lebih dari empat puluh negara di seluruh dunia. Dalam penelitian ini, peneliti menggunakan berbagai tahapan yang selaras dengan framework ISO 31000 [6]. Tahapan-tahap ini digunakan untuk mengumpulkan data dan informasi yang relevan untuk penelitian pada Sistem PENMABA Universitas Sebelas April. Peneliti menggunakan pendekatan dari pihak internal penelitian, yang melibatkan wawancara untuk mengumpulkan data primer dari narasumber.

Untuk mengumpulkan data untuk penelitian ini, kami melakukan wawancara dengan bagian teknologi informasi di Universitas Sebelas April Sumedang. Dengan demikian, peneliti dapat memutuskan penilaian risiko, juga dikenal sebagai penilaian risiko. Penilaian risiko adalah metode yang umum digunakan oleh bisnis dan organisasi untuk menentukan risiko. Penilaian risiko membutuhkan beberapa langkah.



International Organization for Standardization (ISO) 31000 seperti yang ditunjukkan pada gambar diatas, merupakan standar yang disusun dengan tujuan memberikan prinsip dan pedoman manajemen risiko secara universal. Tujuan dari diterapkannya ISO 31000 adalah untuk memberikan pedoman dan prinsip manajamen resiko yang di akui dengan lingkup universal [7]. Tahap pertama yang dilakukan untuk menganalisa adalah Risk Assesment (Penilaian Resiko). Dalam proses ini memiliki 3 tahap yaitu Risk Identification (Identifikasi Resiko), Risk Analys

(Analisis Resiko), dan Risk Evaluation (Evaluasi Resiko). Tahap Risk Assesment (Penilaian Resiko) merupakan proses untuk menentukan potensi resiko yang akan mempengaruhi perusahaan untuk mencapai tujuan bisnis [8]. Proses analisis resiko merupakan proses evaluasi terhadap tingkat kepentingan resiko berdasarkan kriteria yang akan ditentukan Tahap kedua dari manajemen resiko adalah Risk Treatment (Perlakuan Resiko). Tahap ini dilakukan peneliti untuk menyeleksi kemungkinan-kemungkinan resiko, mengurangi, bahkan menghilangkan dampak serta kemungkinan terjadinya resiko yang akan muncul.

HASIL DAN PEMBAHASAN

1. Risk Assessment

Tahapan ini dilakukan untuk mengetahui potensi risiko yang akan mempengaruhi aplikasi dalam penggunaannya. Pada tahap risk assessment ini dilakukan 3 tahap untuk menganalisis sesuai dengan pedoman manajemen risiko ISO 31000 yang meliputi tahap identifikasi risiko (risk identification), analisis risiko (risk analys), dan evaluasi risiko (risk evaluation).

a. Tahap Risk Identification Tahap pertama ini, yang harus dilakukan adalah identifikasi asset yang berhubungan dengan Sistem PENMABA Universitas Sebelas April Sumedang. Dan dalam identifikasi ini melibatkan atau mewawancarai seseorang (salah satu admin PENMABA).

Tabel 3.1 Identifikasi Aset

Komponen Sistem Informasi	Aset MPP Sumedang
Software	Sistem PENMABA Unsap Sumedang
Data	Data dan Informasi
Hardware	PC, Database server, Network devices

Setelah melakukan identifikasi risiko yang menghasilkan informasi dari data, software, dan Hardware yang beruhubungan dengan Sistem PENMABA Universitas Sebelas April Sumedang, maka selanjutnya perlu dilakukan identifikasi kemungkinan - kemungkinan risiko yang mengancam Sistem PENMABA Universitas Sebelas April Sumedang.

Tabel 3.2 Identifikasi Kemungkinan Risiko

Faktor	ID	Kemungkinan Risiko
Alam/Lingkungan	R001	Bencana Alam
	R002	Kebakaran

	R003	Pemadaman Listrik
Manusia	R004	Cybercrime
	R005	Human Error
	R006	Kesalahan Input Data
	R007	Overload
	R008	Penyalahgunaan Hak Akses
Sistem Dan Infrastruktur	R009	Jaringan Bermasalah
	R010	Kerusakan Hardware
	R011	Data Corrupt
	R012	Sever Down
	R013	Maintenance Tidak Terjadwal

Dari tahapan identifikasi risiko, ditemukan ada 13 kemungkinan – kemungkinan risiko yang berasal dari ketiga faktor tersebut yang mengancam Sistem PENMABA Universitas Sebelas April Sumedang. Setelah di ketahui kemungkinan risikonya kemudian melakukan indentifikasi dampak - dampak dari kemungkinan-kemungkinan risiko tersebut.

Tabel 3.3 Identifikasi Dampak Risiko

ID	Kemungkinan Risiko	Dampak
R001	Bencana Alam	Aktivitas kegiatan terganggu
R002	Kebakaran	Kerusakan infrastruktur dan aktivitas layanan terhenti
R003	Pemadaman Listrik	Aktivitas kegiatan terhenti dan terhambat
R004	Cybercrime	Pencurian data
R005	Human Error	Data sulit untuk diakses
R0	Kesalahan Input Data	Menyebabkan ketidakcocokan informasi dan

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

06		data
R007	Overload	Proses terhambat
R008	Penyalahgunaan Hak Akses	Mnipulasi data, kbocoran data dan informasi
R009	Jaringan Bermasalah	Gagal update data, Pelayanan terganggu
R010	Kerusakan Hardware	Kehilangan data
R011	Data Corrupt	Data rusak, Kehilangan data
R012	Sever Down	Kehilangan data, Menghambat Pelayanan, Kerugian
R013	Maintenance Tidak Terjadwal	Sering terjadi error

b. Tahap Risk Analys

Setelah melakukan tahap identifikasi risiko, tahap selanjutnya yaitu tahap analisis risiko. Pada tahap ini dilakukan penilaian terhadap kemungkinan risiko yang telah diidentifikasi. Pada Sistem PENMABA Universitas Sebelas April Sumedang ini, kriteria pengukuran nilai/bobot untuk frekuensi kejadian dan dampak yang diakibatkan dapat dilihat pada table 3.4.

Tabel 3.4 Nilai/Bobot Frekuensi Kejadian dan Dampak Risiko

Frekuensi Kejadian		Dampak yang Diakibatkan	
Nilai	Keterangan	Nilai	Keterangan
(1)	(2)	(3)	(4)
1	Sangat Jarang Terjadi	1	Sangat Kecil
2	Jarang Terjadi	2	Kecil
3	Bisa Terjadi	3	Biasa
4	Sering Terjadi	4	Besar
5	Sangat Sering Terjadi	5	Sangat Besar

Langkah selanjutnya dilakukan penilaian dan pembobotan setiap risiko dari masing-masing kemungkinan risiko tersebut berdasarkan pengelompokan frekuensi kejadian

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

dan dampak yang diakibatkan untuk setiap risiko yang telah diidentifikasi

Tabel 3.5 Penilaian Kemungkinan Risiko

ID	Kemungkinan Risiko		Likelihood	Impact	Evaluasi Risiko
R001	Bencana Alam		1	5	Medium
R002	Kebakaran		1	5	Medium
R003	Pemadaman Listrik		2	3	Medium
R004	Cybercrime		5	5	High
R005	Human Error		2	4	Medium
R006	Kesalahan Input Data		3	3	Medium
R007	Overload		2	4	Medium
R008	Penyalahgunaan Hak Akses		2	3	Medium
R009	Jaringan Bermasalah		3	4	High
R010	Kerusakan Hardware		3	3	Medium
R011	Data Corrupt		4	5	High
R012	Sever Down		5	3	High
R013	Maintenance Tidak Terjadwal		3	4	High

c. Tahap Risk Evaluation

Tahap terakhir dalam risk assesment adalah tahap evaluasi risiko. Dalam tahap ini menggunakan acuan berupa matriks risiko, dimana dalam matriks tersebut dibedakan kedalam 3 risk level yaitu low, medium dan high. Kemungkinan risiko yang telah ditentukan nilai likehood dan nilai impact pada proses sebelumnya akan dibedakan lagi menyusuaikan matriks yang ada.

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

Tabel 3.6 Level Risiko

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

Hasil dari risk evaluation dimana dari 13 kemungkinan risiko terdapat 5 (Cybercrime, Jaringan Bermasalah, Data Corrupt, Sever Down, dan Maintenance Tidak Terjadwal) merupakan level of risk dengan tingkatan high, tardapat risiko lainya sejumlah 8 (Bencana Alam, Kebakaran, Pemadaman Listrik, Human Error, Kesalahan Input Data, Overload, Penyalahgunaan Hak Akses, Kerusakan Hardware) merupakan level of risk tingakatan medium dibedakan kedalam 3 risk level yaitu low, medium dan high. Kemungkinan risiko yang telah ditentukan nilai likehood dan nilai impact pada proses sebelumnya akan dibedakan lagi menysuaikan matriks yang ada.

Tabel 3.6 Level Risiko

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

Hasil dari risk evaluation dimana dari 13 kemungkinan risiko terdapat 5 (Cybercrime, Jaringan Bermasalah, Data Corrupt, Sever Down, dan Maintenance Tidak Terjadwal) merupakan level of risk dengan tingkatan high, tardapat risiko lainya sejumlah 8 (Bencana Alam, Kebakaran, Pemadaman Listrik, Human Error, Kesalahan Input Data, Overload, Penyalahgunaan Hak Akses, Kerusakan Hardware) merupakan level of risk tingakatan medium.

2. Risk Treatment

Setelah melakukan tahap identifikasi risiko, langkah selanjutnya yaitu perlakuan risiko. Pada tahap ini yaitu memberikan saran mengenai perlakuan risiko untuk kemungkinan risiko

yang ada pada Sistem PENMABA Universitas Sebelas April Sumedang. Diharapkan dapat mengurangi dan digunakan untuk pencegahan terhadap kemungkinan risiko yang mungkin akan muncul.

Tabel 3.8 Perlakuan Risiko Terhadap Kemungkinan Risiko

ID	Kemungkinan Risiko	Risk Level	Perlakuan Risiko
R4	Cybercrime	High	Perningkatan keamanan sistem dengan menggunakan firerwall, ernkripsi data sensitif, pelatihan bagi staf untuk mengidentifikasi ancaman siber, serta pemantauan aktif terhadap aktivitas mencurigakan[9]
R9	Jaringan Bermasalah		Permantauan aktif terhadap kesehatan jaringan, pemulihan cepat melalui backup yang teratur, dan mengganti ISP (Internert Servicer Proider) dengan yang baru [10].
R11	Data Corrupt		Melakukan backup data secara berkala.
R12	Sever Down		Pemantauan aktif terhadap kesehatan server, melakukan pengecekan secara berkala dalam 1 hari terhadap db log, temp db log, CPU usage, dan RAM [11].
R13	Maintenance Tidak Terjadwal		Melakukan penjadwalan maintenance rutin setiap minggu [10].
R1	Bencana Alam	Medium	Mensosialisasikan mitigasi bencana alam, dan selalu untuk mengecek informasi di media sosial terkait berita terbaru bencana alam yang terjadi [12].
R2	Kebakaran		Instalasi sistem deteksi dan pemadaman kebakaran, serta persiapan untuk rencana evakuasi yang terstruktur dan pemulihan bencana yang komprehensif [13].
R3	Pemadaman Listrik		Menyediakan generator set listrik dengan daya yang sesuai dengan kebutuhan. Kemurdian menyiapkan Urninterruptible Power Supply (UrPS) [13].
R5	Human Error		Mengadakan daily meeting untuk follow up staff yang mermiliki perrforma yang kurang dari serharusnya, diawali dengan diskusi lalu

			menerapkan kebijakan kampus terkait hal tersebut [12].
R6	Kesalahan Input Data		Melakukan pengecekan secara berkala terhadap data yang salah dalam pengimputan [11].
R7	Overload		Melakukan rerfresh database log, temp dan RAM setelah itu lakukan pengecekan secara teratur minimal seminggu sekali agar tidak adanya penumpukan masalah pada aplikasi [14].
R8	Penyalahgunaan Hak Akses		Memberikan batasan akses pada setiap urser [13].
R10	Kerusakan Hardware		Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan [15].

Tabel 3.9 Evaluasi Hasil Mitigasi Risiko

ID	Kemungkinan Risiko	Likelihood	Impact	Evaluasi Risiko
R001	Bencana Alam	1	3	Low
R002	Kebakaran	1	2	Low
R003	Pemadaman Listrik	1	2	Low
R004	Cybercrime	1	4	Medium
R005	Human Error	3	2	Low
R006	Kesalahan Input Data	2	2	Low
R007	Overload	2	2	Low
R008	Penyalahgunaan Hak Akses	1	2	Low
R009	Jaringan Bermasalah	1	4	Medium
R0	Kerusakan Hardware	2	2	Low

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

10				
R011	Data Corrupt	1	4	Medium
R012	Sever Down	2	4	Medium
R013	Maintenance Tidak Terjadwal	2	3	Medium

Tabel 3.10 Sebelum dan Sesudah Treatment

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

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

3. Monitoring dan Review

Setelah melakukan semua langkah diatas tahap terakhir yaitu melakukan monitoring dan review terhadap hasil kemungkinan risiko dan perlakuan penangannya sehingga segala aktivitas yang akan dilakukan berjalan dengan baik dan lancar, atau setidaknya apabila kemungkinan tersebut terjadi pengguna sudah tau bagaimana cara untuk mencegah dan menanggulangi kemungkinan risiko tersebut. Sebaiknya pengguna melaporkan setiap permasalahan yang terjadi sehingga apabila telah terbentuk kerja sama, risiko yang memungkinkan terjadi dapat cepat teratasi.

KESIMPULAN

Bedasarkan penelitian Evaluasi Risiko Sistem PENMABA Universitas Sebelas April Sumedang, proses manajemen risiko menggunakan ISO 31000:2018, dengan komunikasi dan konsultasi sebagai tahap pertama. Pada tahap kedua, ruang lingkup, konteks, dan standar ditetapkan. Tahap ketiga adalah penilaian risiko, yang terdiri dari identifikasi risiko, analisis risiko, dan evaluasi risiko. Tahap keempat adalah perlakuan risiko. Dari hasil penilaian risiko, yang terdiri dari identifikasi risiko, analisis risiko, dan evaluasi risiko, ditemukan 13 kemungkinan risiko terdapat 5 (Cybercrime, Jaringan Bermasalah, Data Corrupt, Sever Down, dan Maintenance Tidak Terjadwal) merupakan level of risk dengan tingkatan high, tardapat risiko lainya sejumlah 8 (Bencana Alam, Kebakaran, Pemadaman Listrik, Human Error, Kesalahan Input Data, Overload, Penyalahgunaan Hak Akses, Kerusakan Hardware) merupakan level of risk tingakatan medium.

Pada Sistem PENMABA Universitas Sebelas April Sumedang, hasil evaluasi menghasilkan rekomendasi penanganan risiko yang dapat digunakan untuk mengurangi, meminimalkan, dan mencegah ancaman. Jadi, untuk mengurangi risiko yang akan datang, Sistem PENMABA harus diperlakukan dengan benar. Sekurang-kurangnya risiko dapat dikelola dan ditangani sesuai dengan hasil perlakuan yang sudah ditentukan sebelumnya dengan menggunakan struktur ISO 31000:2018.

DAFTAR PUSTAKA

[1] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi Pada Website Ecofo Menggunakan Iso 31000," *Journal Of Computer Science And Engineering (Jcse)*, Vol. 1, No. 2, Pp. 128–146, Aug. 2020, Doi: 10.36596/Jcse.V1i2.76.

[2] D. Yudha Andika And A. Fritz Wijaya, "Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000:2018 Pada Pt. Trust Lerinvital Timur," 2022.

[3] D. P. Natalie And A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Dengan Iso 31000:2018 Pada Pt Bayu Buana Tbk," *Jurikom (Jurnal Riset Komputer)*, Vol. 9, No. 5, P. 1290, Oct. 2022, Doi: 10.30865/Jurikom.V9i5.4797.

[4] D. Made, D. U. Putra, G. S. Mahendra, And E. Mulyadi, "Sistem Informasi Penerimaan Siswa Baru Pada Smp Negeri 3 Cibal Berbasis Web," *Insert: Information System And Emerging Technology Journal*, Vol. 3, No. 1, 2022.

[5] 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

[6] J. Rohman And E. Fadilah, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000 Pada Sistem Komputerisasi Haji Terpadu Di Kantor Kementerian Agama Kabupaten Ogan Ilir."

[7] Z. Munawwaroh, U. Syarif, And H. Jakarta, "Analisis Manajemen Risiko Pada Pelaksanaan Program Pendidikan Dalam Upaya Meningkatkan Mutu Pendidikan," *Jurnal Administrasi Pendidikan*, No. 2, 2017.

[8] 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.

[9] D. R. Yuniarti, H. F. Alfarizy, Z. Siallagan, And M. W. Rizkyanfi, "Analisis Potensi Dan Strategi Pencegahan Cyber Crim Dalam Sistem Logistik Di Era Digital," *Jurnal Bisnis, Logistik Dan Supply Chain (Blogchain)*, Vol. 3, No. 1, Pp. 23–32, Jun. 2023, Doi: 10.55122/Blogchain.V3i1.714.

[10] E. Muryanti And K. D. Hartomo, "Analisis Risiko Teknologi Informasi Aplikasi Catter Pdam Kota Salatiga Menggunakan Iso 31000," 2021. [Online]. Available: Http://Jurnal.Mdp.Ac.Id

[11] E. Saputra, C. Rudianto, And F. Tanaem, "Analisis Resiko Sistem Informasi Penjualan Berbasis Iso 31000: Study Kasus Pt Xyz," 2022.

[12] 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.

[13] P. Kanantyo, F. S. Papilaya, K. S. Wacana, J. Blotongan, K. Salatiga, And J. Tengah, "Analisis Risiko Teknologi Informasi Menggunakan Iso 31000 (Learning Management System Smpn 6 Salatiga)," 2021. [Online]. Available: Http://Jurnal.Mdp.Ac.Id

[14] D. Junianti And C. Fibriani, "Analisis Resiko Aplikasi Sistem Informasi Pengelolaan Data Umat Menggunakan Iso 31000 (Studi Kasus: Gereja Katolik Santo Paulus Miki Salatiga)," 2021. [Online]. Available: Https://Journal-Computing.Org/Index.Php/Journal-Cisa/Index

[15] I. Setiawan, A. R. Sekarini, R. Waluyo, And F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan Iso 31000 Dan Standar Pengendalian Iso/Eic 27001 Di Tripio Purwokerto," *Matrik : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, Vol. 20, No. 2, Pp. 389–396, May 2021, Doi: 10.30812/Matrik.V20i2.1093.