Jurnal Riset Teknik Informatika (JURETI)
Vol. x, No. y, Agustus 2024, pp. x-y

DOI: .. . ./jureti
p-ISSN: XXXX-XXXX
e-ISSN: XXXX-XXXX

IMPLEMENTATION OF ISO 31000:2018 FOR RISK MANAGEMENT IN SISTEM INFORMASI AKADEMIK (SIAKAD) AT SEBELAS APRIL UNIVERSITY

Arini Fitrian Rebitasari[1], Dwi Yuniarto[2], David Setiadi[3]

[12,3]Informatics, Faculty of Information Technology, Sebelas April University Sumedang
Email: [1]a2.2000013@mhs.stmik-sumedang.ac.id, [2]dwiyuniarto@unsap.ac.id , [3]david@unsap.ac.id

(Article received: date; Revision: date; published: date)

Abstract

Sistem Informasi Akademik (SIAKAD) began operating in 2020 and has proven to be very helpful for lecturers, staff and students in their lecture activities. Even though it provides many benefits, this system also carries risks in the form of threats that can harm its users. This research aims to reduce existing and possible risks that may arise in the future, as well as provide appropriate recommendations for handling risks related to Sistem Informasi Akademik at Sebelas April University. Risk analysis is carried out using an approach using the Control Objectives for Information and Related Technologies 5 for Risk method and the ISO 31000:2018 standard. Based on risk analysis of information technology in the Academic Information System at Sebelas April University Sumedang, which was carried out using the Control Objectives for Information and Related Technologies 5 for Risk and International Organization for Standardization 31000:2018 methods as well as interviews with related sources, 13 potential risks were found that could occurs and threatens 4 types of Information Technology resources (Application, Information, Infrastructure, and People). Of the 13 risks, 12 risks are in the High category, namely system hacking, system crash, virus attack, overload, loss of current data, data theft, database error, hardware damage, server down, unstable network connection, human error, and misuse of position. Meanwhile, 1 other risk is in the medium category, namely Natural Disasters. This risk condition indicates the need for risk management, and by using the International Organization for Standardization 31000 framework and Control Objectives for Information and Related Technologies 5 for Risk, these risks can be managed and handled in accordance with previously determined treatment.

Keywords: Risk Analysis, Sistem Informasi Akademik (SIAKAD), ISO 31000:2018, COBIT 5 for risk.

PENERAPAN ISO 31000:2018 UNTUK MANAJEMEN RISIKO PADA SISTEM INFORMASI AKADEMIK DI UNIVERSITAS SEBELAS APRIL SUMEDANG

Abstrak

Sistem Informasi Akademik mulai beroperasi pada tahun 2020 dan terbukti sangat membantu dosen, staf, dan mahasiswa dalam aktivitas perkuliahan. Meskipun memberikan banyak manfaat, sistem ini juga membawa risiko berupa ancaman yang dapat merugikan penggunanya. Penelitian ini bertujuan untuk mengurangi risiko yang ada maupun yang mungkin timbul di masa depan, serta memberikan rekomendasi yang tepat untuk menangani risiko terkait Sistem Informasi Akademik di Universitas Sebelas April. Analisis risiko dilakukan dengan pendekatan menggunakan metode Control Objectives for Information and Related Technologies 5 for Risk dan standar ISO 31000:2018. Berdasarkan analisis risiko terhadap teknologi informasi pada Sistem Informasi Akademik di Universitas Sebelas April Sumedang, yang dilakukan menggunakan metode Control Objectives for Information and Related Technologies 5 for Risk dan International Organization for Standardization 31000:2018 serta wawancara dengan narasumber terkait, ditemukan 13 potensi risiko yang dapat terjadi dan mengancam 4 jenis sumber daya Teknologi Informasi (Application, Information, Infrastruktur, dan People). Dari 13 risiko tersebut, 12 risiko berada dalam kategori High, yaitu peretasan sistem, sistem crash, serangan virus, overload, hilangnya data terkini, pencurian data, database eror, kerusakan hardware, server down, Koneksi jaringan tidak stabil, human eror, dan penyalahgunaan kedudukan. Sedangkan 1 risiko lainnya berada dalam kategori Medium, yaitu Bencana Alam. Kondisi risiko ini menunjukkan perlu adanya pengelolaan risiko ini, dan dengan menggunakan framework International Organization for Standardization 31000 dan Control Objectives for Information and Related Technologies 5 for Risk, risiko-risiko tersebut dapat dikelola dan ditangani sesuai dengan perlakuan yang telah ditetapkan sebelumnya.

Kata kunci: *Analisis Risiko, Sistem Informasi Akademik (SIAKAD), ISO 31000:2018, COBIT 5 for risk.*

1. PENDAHULUAN

Peranan teknologi dalam aktivitas manusia sangat besar, sehingga hampir setiap organisasi atau instansi memberikan perhatian khusus terhadap perkembangan teknologi [1]. Universitas Sebelas April merupakan salah satu institusi yang telah menerapkan dan mengembangan teknologi melalui sistem informasi untuk menunjang kegiapan operasionalnya. Ketika sebuah institusi mengandalka pada sistem informasi untuk menjalankan sebagian besar aktivitas bisnisnya, maka risiko menjadi ancaman [2]. Langkah awal dalam mengelola risiko dengan cara melakukan manajemen risiko atau pengukuran terhadap risiko teknologi informasi [3]. Manajemen risiko bertujuan untuk mengenali dan mengelola risiko serta kejadian yang mungkin akan muncul, meminimalkan dampaknya dan menentukan penanganan risiko yang tepat untuk meningkatkan peluang sukses [4]. Proses manajemen risiko ini merupakan salah satu langkah yang dapat diikuti untuk menciptakan perbaikan berkelanjutan [5].

Sistem Informasi Akademik merupakan sistem informasi yang digunakan di Universitas Sebelas April yang dapat menunjang kegiatan perkuliahan yang dapat digunakan oleh mahasiswa, dosen, dan staf. Sistem informasi akademik ini membantu mengelola data dosen dan mahasiswa dengan mudah serta mengelola pelayanan administari akademik seperti Kartu Rencana Studi, Kartu Hasil Studi, input nilai, jadwal perkuliahan secara online. Sistem Informasi Akademik sudah digunakan sejak tahun 2020. Sistem ini dinilai sangat membantu dosen, pegawai dan mahasiswa dalam melakukan aktivitasnya. Tidak hanya memberikan manfaat bagi penggunanya, akan tetapi Sistem Informasi Akademik juga menimbulkan beberapa permasalahan yang dapat menggangu proses bisnis serta dapat merugikan para pengguna.

Penelitian ini bertujuan untuk mencegah atau mengurangi segala kemungkinan dan permasalahan yang sedang dialami maupun yang akan terjadi serta memberikan rekomendasi yang tepat bagi Sistem Informasi Akademik di Universitas Sebelas April. Manajemen risiko ini dilakukan dengan menggunakan pendekatan metode COBIT 5 for risk dan ISO 31000:2018.

International Organization for Standardization (ISO) 31000:2018 adalah pendekatan yang umum digunakan dalam manajemen risiko [6]. Standar ini terdiri dari tiga komponen utama, yaitu prinsip, kerangka kerja, dan proses manajemen risiko. Prinsipnya memberikan pedoman tentang bagaimana manajemen risiko dapat dilakukan dengan cara yang efektif dan efisien [7]. Kerangka kerjanya membantu dalam mengintegrasikan manajemen risiko ke dalam aktivitas dan fungsi organisasi [8]. Sementara itu, prosesnya mencakup penerapan sistematis dari kebijakan, prosedur, dan praktik dalam aktivitas manajemen risiko [9]. Perusahaan menerapkan ISO 31000:2018 untuk menciptakan dan melindungi nilai perusahaan dengan mengelola risiko dalam setiap perencanaan dan pengambilan keputusan, serta mendukung peningkatan kinerja perusahaan [10].

COBIT 5 merupakan kerangka kerja yang dirancang untuk membantu organisasi dalam mencapai tujuan dan sasaran melalui tata kelola dan manajemen teknologi informasi [11]. COBIT 5 for risk merupakan bagian dari COBIT 5 yang fokus pada manajemen risiko. Risk appetite mengacu pada tingkat dan jenis risiko yang ebrsdia diterima oleh organisasi, sehingga tidak semua risiko perlu dihindari. Ini dicapai dengan menetapkan batas maksimum terhadap risiko pada beberapa kategori proses bisnis yang mengandung risiko teknologi informasi, yang digunakan untuk mencapai tujuan perusahaan [12].

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif, yang menghasilkan data berupa pertanyaaan-pertanyaan yang mengangkat isu, persoalan, atau tantangan yang relevan dengan situasi, kondisi dan kenyataan yang ada. Temuan dari penelitian kualitatif inin akan digunakan sebagai bahan untuk dianalisis lebih lanjut dalam rangka mendapatkan solusi pesmasalahan yang dihadapi oleh Sistem Informasi Akademik di Universitas Sebelas April.

Teknik pengumpulan data yang diterapkan adalah wawancara. Dalam hal ini, wawancara ditujukan kepada admin Sistem Informasi Akademik yang berada di bidang Informatika, dengan tujuan untuk mengidentifikasi risiko-risko yang mungkin muncul pada Sistem Informasi tersebut.

Selain menggunakan metode wawancara, metode lain yang digunakan ialah metode analisis manajemen risiko berdasarkan ISO 31000:2018. Berikut adalah langkah-langkah utama dalam proses manajemen risiko secara garis besar:

Gambar 1. Metode Penelitian

Berdasarkan gambar 1 diatas, maka dapat dijelaskan sebagai berikut:

- Identifikasi Sumber Daya TI
  Proses ini mencakup pengidentifikasian potensi risiko yang mungkin timbul dalam suatu aktivitas usaha. Identifikasi risiko yang tepat dan menyeluruh sangat penting dalam manajemen risiko. Salah satu langkah kunci dalam identifikasi risiko adalah mencatat sebanyak mungkin risiko yang mungkin terjadi.

- Analisis Risiko
  Analisis Risiko dilakukan dengan memberikan nilai dari setiap risiko yang teridentifikasi. Setiap risiko dinilai berdasarkan frekuensi kemunculan dan dampak yang dihasilkan.
- Evaluasi Risiko
  Proses ini digunakan untuk menetapkan strategi manajemen risiko dengan membandingkan tingkat risiko yang ada dengan standar telah ditetapkan, target tingkat risiko dan kriteria lainnya.
- Perlakuan Risiko
  Penanganan risiko melibatkan upaya untuk menentukan strategi untuk mengelola risikorisiko yang telah diidentifikasi, dianalisis, dan dievaluasi sebelumnya Perlakuan risiko adalah usaha dalam menentukan strategi perlakuan terhadap risiko-risiko yang telah diidentifikasi, dianalisis, dan dievaluasi sebelumnya. Terdapat empat jenis strategi perlakuan risiko, diantaranya: Risk Avoidauce (Menghindari Risiko), Risk Reduction (Mengurangi/Mitigasi Risiko), Risk Sharing (Membagi Risiko), dan Risk Acceptance (Menerima Risiko). Dalam penelitian ini, peneliti memilih strategi perlakuan risiko yaitu Risk Reduction (Mengurangi/Mitigasi Risiko).
- Pemantauan dan Tinjauan
  Pemantauan adalah proses rutin untuk mengevaluasi kinerja aktual manajemen risiko dibandingkan dengan rencana atau ekspetasi yang telah ditetapkan. Tinjauan adalah evaluasi berkala terhadap kondisi saat ini dengan fokus tertentu, seperti efektivitas kontrol terhadap risiko untuk menyempurnakan analisis risiko yang ada.

3. HASIL DAN PEMBAHASAN

3.1 Identifikasi Risiko

Tahap ini dilakukan identifikasi sumber daya TI pada Sistem Informasi Akademik Universitas Sebelas April. Setelah dilakukan identifikasi sumber daya TI yang berkaitan dengan Sistem Informasi Akademik. Selanjutnya adalah mengidentifikasi untuk kemungkinan risiko yang mungkin menjadi risiko atas keberadaan sumber daya TI Sistem Informasi Akademik yang berasal dari beragam.

Tabel 1 Sumber Daya TI

No	Sumber Daya TI	
1	***Application***	Sistem Informasi Akademik
2	***Information***	Data dan informasi akademik
3	***infrastructure***	*IP public, server,share hosting, PC*
4	***people***	Super admin, operator, pengguna

Tabel 2 Identifikasi Risiko

No	Sumber Daya TI	Identifikasi Risiko
1	**Application**	**1. Peretasan sistem**
		2. Sistem *crash*
		3. Serangan virus
		4. Overload
2	**Information**	**5. Hilangnya data terkini**
		6. Pencarian data
		7. Database eror
3	**Infrastructure**	**8. Kerusakan hardware**
		9. Server down
		10. Koneksi jaringan tidak stabil
		11. Bencana alam
4	**People**	**12. Human eror**
		13. Penyalahgunaan hak akses

Hasil dari proses identifikasi risiko pada tabel 2 diatas, menunjukan adanya 13 potensi risiko yang berasal dari sumber daya TI yaitu *application, information, infrastructure,* dan *people* yang dapat mempengaruhi sistem. Selanjutnya, risiko- risiko yang telah diidentifikasi tersebut dianalisis untuk menilai dampaknya terhadap sistem. Dengan demikian, di dalam proses ini dampak dari setiap risiko yang ada dapat diidentifikasi.

3.2 Analisis Risiko

Pada tahap ini, dilakukan penilaian terhadap potensi risiko yang muncul dengan mempertimbangkan frekuensi kemunculan risiko dan tingkat dampat yang diakibatkan oleh masing-masing risiko. Dalam penelitian ini, kriteria untuk menilai frekuensi risiko dan tingkat dampak yang ditimbulkan bisa dilihat pada Tabel berikut.

Tabel 3 Nilai Frekuensi dan Dampak Kejadian

Frekuensi kejadian		Dampak yang diakibatkan	
Nilai	**Keterangan**	**Nilai**	**Keterangan**
1	Sangat jarang terjadi	1	Sangat jarang terjadi
2	Jarang terjadi	2	Jarang terjadi
3	Biasa terjadi	3	Biasa terjadi
4	Sering terjadi	4	Sering terjadi
5	Sangat sering terjadi	5	Sangat sering terjadi

Selanjutnya, setiap risiko yang telah diidentifikasi diberikan nilai berdasarkan frekuensi kemunculannya dan dampak yang dihasilkannya. Detail hasil penilaian risiko dapat ditemukan pada tabel berikut.

Tabel 4 Penelitian Identifikasi Risiko Menurut Frekuensi Dan Dampak

No	IT resources	Identifikasi Risiko	Frekuensi	Dampak
1	***Application***	Peretasan sistem	**2**	**5**
		Sistem crash	**3**	**4**
		Serangan virus	**3**	**4**
		Overload	**2**	**5**

2	***Information***	Hilangnya data terkini	**2**	**5**
		Pencurian data	**2**	**5**
		Database eror	**3**	**5**
3	***Infrastructure***	Kerusakan hardware	**2**	**5**
		Server down	**5**	**5**
		Koneksi jaringan tidak stabil	**5**	**4**
		Bencana alam	**1**	**4**
4	***People***	Human eror	**5**	**4**
		Penyalahgunaan kedudukan	**5**	**4**

3.3 Evaluasi Risiko

Evaluasi risiko dilakukan melalui pemetaan grafik (x,y) yang menggambarkan hubungan antara frekuensi kemunculan risiko dan tingkat dampak yang ditimbulkan oleh masing-masing risiko. Hasil dari evaluasi ini dikelompokan ke dalam tiga kategori yaitu *Low, Medium,* dan *High*, berdasarkan kombinasi intensitas dan dampaknya.

Tabel 5 Matriks Evaluasi Risiko

Frekuensi	**Dampak**				
	1	**2**	**3**	**4**	**5**
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*

Tabel 6 Matriks Evaluasi Risiko TI Berdasarkan Frekuensi dan Dampak

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

Tabel 6 diatas menunjukan sebaran risiko dari sumber daya TI yang telah diidentifikasi sebelumnya berdasarkan pemetaan antara nilai frekuensi kejadian risiko dengan nilai dampak yang diakibatkan. Berdasarkan pengelompokan kategori evaluasi risiko, jenis risiko yang dihasilkan dari kombinasi nilai frekuensi dan dampak dapat dilihat pada tabel tersebut.

Tabel 7 Evaluasi Risiko Berdasarkan *mapping* Risiko dengan Frekuensi-Dampak

No	**IT Resources**	**Identifikasi Risiko**	**Frekuensi**	**Dampak**	**Evaluasi Risiko**
1	*Application*	Peretasan sistem	2	5	High
		Sistem *crash*	3	4	High
		Serangan virus	3	4	High
		Overload	2	5	High
2	*Information*	Hilangnya data terkini	2	5	High
		Pencurian data	2	5	High
		Database eror	3	5	High
3	*Infrastrucrture*	Kerusakan hardware	2	5	High
		Server down	5	5	High
		Koneksi jaringan tidak stabil	5	4	High
		Bencana alam	1	4	Medium
4	*People*	Human eror	5	4	High
		Penyalahgunaan kedudukan	5	4	High

3.4 Perlakuan Terhadap Risiko

Strategi penanganan risiko yang paling sesuai untuk mengatasi permasalahan dibahas adalah menggunakan Risk Reduction. Program-program penanganan risiko yang dapat diterapkan dapat dilihat pada tabel dibawah ini.

Tabel 8 Penanganan Risiko

No	**IT Resources**	**Identifikasi Risiko**	**Penanganan Risiko**
1	*Application*	Peretasan sistem	Melakukan perbaikan sistem aplikasi dengan memperbarui patch dan menerapkan sistem firewall, serta meningkatkan keamanan sistem secara menyeluruh
		Sistem *crash*	Memperbaiki kesalahan sistem yang ditemukan selama prose pemeliharaan
		Serangan virus	Menyediakan perangkat antivirus dan melakukan pemindaian virus secara berkala pada perangkat komputer
		Overload	Memantau server untuk memastikan kondisinya baik, mengoptimalkan gambar, dan meningkatkan kapasitas bandwidth
2	*information*	Hilangnya data terkini	Melalukan pencadangan data secara berkala sesuai dengan standar dan membatasi hak akses terhadap data
		Pencurian data	Menilai mekanisme keamanan data oleh manajemen puncak
		Database eror	Melakukan backup data secara berkala sesuai standar. Membatasi hak akses terhadap data
3	*Infrastructure*	Kerusakan hardware	Menetapkan tanggung jawab kepada setiap karyawan untuk menggunakan perangkat keras sesuai prosedur yang berlaku. Jika perangkat keras rusak dan tidak dapat diperbaiki, segera ajukan permintaan untuk perangkat keras baru agar

			tidak menggangu proses bisnis
		Server down	Melakukan pemeriksaan rutin pada database SIAKAD serta melakukan penyegaran pada penggunakan log, file sementara, dan RAM dari SIAKAD dan database utama untuk mencegah terjadianya ganguan server
		Koneksi jaringan tidak stabil	Mengganti ISP (Internet Service Provider) dengan yang lebih baik
		Bencana alam	Pastikan lokasi penyimpanan cadangan memiliki risiko bencana alam yang lebih rendah dibandingkan dengna lokasi penyimpanan data utama.
4	*People*	Human eror	Melakukan training pada setiap SDM yang menggunakan sistem
		Penyalahgunaan kedudukan	Rekam setiap altvotas pegawai sebagai langah pencegahan, sehingga setiap perubahan data dapat diketahui siapa yang melakukan dan kapan perubahan tersebut terjadi

Tabel 9 Evaluasi Mitigasi Risiko

No	IT Resources	Identifikasi Risiko	Frekuensi	Dampak	Evaluasi Risiko
1	*Application*	Peretasan sistem	2	2	Low
		Sistem *crash*	2	2	Low
		Serangan virus	1	2	Low
		Overload	2	2	Low
2	*Information*	Hilangnya data terkini	2	1	Low
		Pencurian data	2	2	Low
		Database eror	3	2	Low
3	*Infrastrucrture*	Kerusakan hardware	2	2	Low
		Server down	4	2	Medium
		Koneksi jaringan tidak stabil	4	2	Medium
		Bencana alam	1	2	Low
4	*people*	Human eror	4	1	Medium
		Penyalahgunaan kedudukan	5	2	Medium

Berdasarkan Tabel 10 diatas, terlihat perubahan dalam area risiko setelah penerapan program penanganan risiko (mitigasi risiko), keberhasilan dari pelaksanaan program tersebut diharapkan menjadi tanggung jawab bersama. Pelaksanaan program penanganan risiko tersebut harus sesuai dengan Standard Operating Procedure Manajemen Risiko yang sudah ditetapkan.

3.5 Pemantauan dan Tinjauan

Pemantauan dan tinjauan sebaiknya dilaksanakan secara bersamaan setiap langkahlangkah dalam proses penilaian risiko diimplementasikan. Proses pemantauan ini harus melibatkan berbagai pihak, termasuk pemangku kepentingan. Ada tiga jenis bentuk pemantauan dan tinjauan yang harus dilakukan terus menerus oleh instansi sebagai bagian dari tanggung jawab pekerjaan pada level jabatan, yaitu:

1) Pemeriksaan rutin dan pemantauan berkelanjutan, yang dilakukan setiap hari sebagai bagian dari tugas sehari-hari.
2) Pemeriksaan oleh atasan, yang dilakukan secara periodik dan didorong oleh profil risiko serta tanggungjawab pejabat terkait.
3) Audit oleh pihak ketiga, yang melibatkan verifikasi oleh auditor internal dan eksternal untuk menilai kepatuhan terhadap standar dan peraturan yang berlaku.

4. DISKUSI

Dari penelitian yang dilakukan, ditemukan 13 potensi risiko yang mungkin terjadi. Menurut Bisma R, penanganan risiko terkait serangan virus melibatkan penyediaan antivirus dan pemindaian virus secara rutin pada perangkat komputer. Sebaliknya, peneliti lain menyarankan untuk menangani risiko serangan virus dengan melakukan pemindaian antivirus pada perangkat portabel, serta selalu mengaktifkan firewall dan keamanan internet. Fathoni M merekomendasikan untuk mengatasi risiko kesalahan database dengan melakukan pencadangan data secara berkala sesuai standar dan membatasi hak akses data. Namun, peneliti lain berpendapat bahwa penanganan kesalahan database juga melibatkan pembaruan perangkat lunak database dan sistem operasi secara teratur untuk mengatasi bug, serta pemeliharaan rutin seperti pengoptimalan kueri dan indeks untuk meningkatkan kinerja database. Butarbutar N mengusulkan perbaikan server down melalui pembaruan sistem aplikasi dengan patch terbaru dan penerapan firewall, disertai dengan peningkatan keamanan sistem. Peneliti lain menambahkan bahwa penanganan server down harus mencakup kebijakan pengecekan server secara berkala dan jadwal pemeliharaan atau pembaruan server yang jelas. Untuk mengatasi risiko kesalahan manusia, Sitanggang P menyarankan pelatihan bagi setiap sumber daya manusia yang menggunakan sistem sebagai langkah pencegahan. Peneliti lain mengusulkan pembagian tugas kepada karyawan sesuai kemampuan mereka dan pembuatan serta penerapan SOP untuk memperjelas peraturan di bidang pekerjaan mereka.

5. KESIMPULAN

Berdasarkan analisis risiko terhadap teknologi informasi pada Sistem Informasi Akademik di

Universitas Sebelas April Sumedang, yang dilakukan menggunakan metode COBIT 5 for Risk dan ISO 31000:2018 serta wawancara dengan narasumber terkait, ditemukan 13 potensi risiko yang dapat terjadi dan mengancam 4 jenis sumber daya TI (Application, Information, Infrastruktur, dan People). Dari 13 risiko tersebut, 12 risiko berada dalam kategori High, yaitu peretasan sistem (R1), sistem crash (R2), serangan virus (R3), overload (R4), hilangnya data terkini (R5), pencurian data (R6), database eror (R7), kerusakan hardware (R8), server down (R9), Koneksi jaringan tidak stabil (R10), human eror (R12), dan penyalahgunaan kedudukan (R13). Sedangkan 1 risiko lainnya berada dalam kategori Medium, yaitu Bencana Alam (R11). Kondisi risiko ini menunjukkan perlu adanya pengelolaan risiko ini, dan dengan menggunakan framework ISO 31000 dan COBIT 5 for Risk, risiko-risiko tersebut dapat dikelola dan ditangani sesuai dengan perlakuan yang telah ditetapkan sebelumnya.

Untuk manajemen risiko pada Sistem Informasi Akademik di Universitas Sebelas April, diperlukan tindakan untuk mengurangi kemungkinan risiko dengan menindaklanjuti perlakuan risiko secara efektif agar proses bisnis berjalan sesuai harapan. Penelitian ini menunjukkan bahwa aset yang diteliti belum lengkap, sehingga disarankan untuk penelitian di masa depan agar memiliki cakupan lebih luas, termasuk pemanfaatan IoT (Internet of Things) atau AI (Artificial Intelligence) untuk mencegah, mengatasi alternatif solusi risiko, dan menyelesaikan risiko yang ada. Hal ini akan membantu pemangku kepentingan dalam menyusun dokumentasi terkait manajemen risiko sesuai dengan tren terkini.

Kesimpulan merupakan inti dari keseluruhan paper. Dibuat dalam bentuk paragraph, dan tidak dalam bentuk list. Kesimpulan tidak mengulang kalimat yang ada di dalam abstrak.

6. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah membantu dalam proses penelitian ini. Kepada dosen pembimbing yang sudah mengarahkan dan memberikan saran kepada penulis dalam menyelesaikan penelitian ini.

7. DAFTAR PUSTAKA

[1] J. N. Utamajaya, A. Afrina, and A. N. Fitriah, "Analisis Manajemen Risiko Teknologi Pada Perusahaan Toko Ujung Pandang Grosir PENAJAM Paser Utara Menggunakan Framework ISO 31000:2018," *Sebatik*, vol. 25, no. 2, pp. 326–334, Dec. 2021, doi: 10.46984/sebatik.v25i2.1430.

[2] M. Ayuningtyas and P. F. Tanaem, "Information Technology Asset Security Risk Management at the Secretariat of the Salatiga City DPRD Using ISO 31000," *Journal of Information Systems and Informatics*, vol. 4, no. 1, 2022, [Online]. Available: http://journal-isi.org/index.php/isi

[3] 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, 2021, [Online]. Available: http://journal-isi.org/index.php/isi

[4] T. F. Rahardian and A. F. Wijaya, "Risk Analysis of Web-Based Information Systems on CV Mega Komputama Uses ISO 31000," *Journal of Information Systems and Informatics*, vol. 4, no. 2, 2022, [Online]. Available: http://journal-isi.org/index.php/isi

[5] 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

[6] 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.

[7] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *Jurnal Riset Komputer*, vol. 7, no. 1, p. 91, Feb. 2020, doi: 10.30865/jurikom.v7i1.1791.

[8] K. Aprianto, Endroyono, and S. M. Susiki Nugroho, "Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000:2018 di Kabupaten Magetan E-Government Risk Management Analysis Using COBIT 5 For Risk and ISO 31000:2018 in Magetan Regency," 2021.

[9] R. Fahlepi, M. Fronita, E. Saputra, M. Luthfi Hamzah, A. Marsal, and S. Daulay, "Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000," 2023.

[10] F. Mahardika, M. Agreindra H, S. A. Fatimah, and L. T. Nur F, "Manajemen Risiko Teknologi Informasi Aplikasi E-Office ASN Menggunakan ISO 31000:2018," *Infotekmesin*, vol. 14, no. 2, pp. 237–243, Jul. 2023, doi: 10.35970/infotekmesin.v14i2.1877.

[11] P. P. Thenu, A. F. Wijaya, and C. Rudianto, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi KAsus: PT Global Infotech)," 2020.

[12] F. A. Kojongian and M. Ayub, "Manajemen Risiko Divisi Sistem Informasi Perguruan Tinggi Dengan Framework COBIT 5," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 7, no. 1, Apr. 2021, doi: 10.28932/jutisi.v7i1.3434.