

Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000

Ridho Fahlepi^{1*}, Mona Fronita², Eki Saputra³, Muhammad Luthfi Hamzah⁴, Arif Marsal⁵, Suandi Daulay⁶

^{1,2,3,4,5}Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia

⁶Sekolah Tinggi Teknologi Pekanbaru, Indonesia

e-mail: ridho.fahlepi68@gmail.com

Abstract

The development of information technology is unavoidable. All aspects of human life require information technology. The use of information technology makes work easier to carry out. However, information technology also poses risks that can threaten the activities of an agency. The Pekanbaru College of Technology (STT) has implemented an Academic Information System (SIKAD) to improve academic administration services, such as managing KRS, KHS, value input, schedules, and payments. Through interviews, it was identified possible risks that could disrupt business processes in the agency. The purpose of this study was to obtain an RPN (Risk Priority Number) value to provide recommendations for risk treatment in the Academic Information System (SIKAD). The method used is ISO 31000 to measure the level of risk. The research stages include risk identification, risk analysis, calculation of RPN values, risk evaluation, and risk treatment. This research produces a level of risk from the highest to the lowest that can be used as a reference in the evaluation, treatment, and recommendations to overcome these risks.

Keywords: Risk Management, Academic Information System (SIKAD), ISO 31000, Risk Priority Number (RPN).

Abstrak

Perkembangan teknologi informasi tidak dapat dihindari. Semua aspek kehidupan manusia membutuhkan teknologi informasi. Penggunaan teknologi informasi membuat pekerjaan semakin mudah dilaksanakan. Namun, teknologi informasi juga menimbulkan risiko yang dapat mengancam aktivitas suatu instansi. Sekolah Tinggi Teknologi (STT) Pekanbaru telah menerapkan Sistem Informasi Akademik (SIKAD) untuk meningkatkan pelayanan administrasi akademik, seperti mengelola KRS, KHS, input nilai, jadwal, dan pembayaran. Melalui wawancara, teridentifikasi kemungkinan risiko yang dapat mengganggu proses bisnis di instansi tersebut. Tujuan penelitian ini adalah untuk mendapatkan nilai RPN (Risk Priority Number) guna memberikan rekomendasi perlakuan risiko pada Sistem Informasi Akademik (SIKAD). Metode yang digunakan adalah ISO 31000 untuk mengukur tingkat risiko. Tahapan penelitian meliputi identifikasi risiko, analisis risiko, penghitungan nilai RPN, evaluasi risiko, dan perlakuan risiko. Penelitian ini menghasilkan tingkat risiko dari yang tertinggi hingga terendah yang dapat digunakan sebagai acuan dalam evaluasi, perlakuan, serta rekomendasi untuk mengatasi risiko tersebut.

Kata kunci: Manajemen Risiko, Sistem Informasi Akademik (SIKAD), ISO 31000, Risk Priority Number (RPN).

1. PENDAHULUAN

Risiko adalah potensi bahaya, yang mengarah pada aktivitas bisnis instansi yang kurang ideal. Risiko adalah sesuatu yang tidak pasti dan mempengaruhi peluang instansi untuk mencapai suatu tujuan atau ambisi [1]. Risiko adalah bagian yang tidak terpisahkan dari aktifitas manusia, ibarat seperti tidak ada kehidupan tanpa adanya risiko [2]. Ketika sistem yang dikerahkan tidak berfungsi

secara efektif, sebuah institusi yang bergantung pada sistem informasi untuk sebagian besar proses bisnisnya dapat mengalami gangguan serius [3]. Jika timbul bahaya dalam penggunaan perangkat lunak dan perangkat keras, instansi harus siap mengambil tindakan yang tepat [4]. Penanganan risiko ditujukan pada aset yang memiliki kemungkinan terjadinya risiko dengan mengidentifikasi penyebab dan mencari solusi yang tepat [5]. Analisis manajemen risiko merupakan suatu proses yang dilakukan pada tingkat manajemen pelaksana, yaitu berupa proses analisis sistematis dari setiap kerugian yang dapat dihadapi oleh sebuah perusahaan, akibat dari suatu risiko juga cara pengendalian yang tepat guna mengatasi kerugian pada instansi [6].

Manajemen risiko teknologi informasi diperlukan untuk mengurangi kemungkinan dan dampak dari potensi risiko berdasarkan potensi tingkat risiko tersebut. Manajemen risiko merupakan kegiatan mengurangi atau mengendalikan kemungkinan kesalahan atau kerugian yang diakibatkan oleh semua risiko [7]. Manajemen risiko harus dilakukan sebagai bagian dari manajemen instansi. Proses manajemen risiko ini merupakan salah satu langkah yang dapat diikuti untuk menciptakan perbaikan berkelanjutan. Selain itu, manajemen risiko adalah proses yang sering dikaitkan dengan pengambilan keputusan di instansi [8]. Dengan demikian keberhasilan manajemen risiko bergantung pada manusia-manusia yang melaksanakannya. Lebih spesifik lagi, keberhasilan manajemen risiko bergantung pada kemampuan (kapabilitas), cara pandang (persepsi), dan niat (intensi) orang-orang yang melaksanakannya [9]. Meskipun risiko tidak dapat sepenuhnya dihilangkan, setidaknya dapat dikelola, menjadikan aset Teknologi Informasi (TI) suatu instansi lebih fungsional dan berguna. Hal ini memungkinkan instansi untuk memperoleh manfaat dari manajemen risiko dengan memastikan bahwa aktivitas bisnis dilakukan secara efisien. Instansi yang maju, pastinya sangat menyadari bahwa pentingnya pengelolaan risiko yang terkait dengan perencanaan serta penerapan TI instansi, sehingga tidak hanya terpaku pada satu sektor tertentu saja, melainkan dari berbagai sektor juga memerlukan manajemen risiko TI dengan baik [10].

Sekolah Tinggi Teknologi (STT) Pekanbaru merupakan instansi yang bergerak dibidang pendidikan yang berada di jalan Dirgantara No.4, Kel, Sidomulyo Timur., Kec. Marpoyan Damai, Kota Pekanbaru, Riau. Berdasarkan wawancara yang telah dilakukan dengan Kepala IT STT Pekanbaru yakni Bapak Suandi Daulay, M.Kom, Instansi sudah menerapkan teknologi informasi dalam aktivitas pelayanan akademik. Adapun teknologi yang diterapkan yaitu Sistem Informasi Akademik (SIKAD) yang memiliki tujuan guna meningkatkan kinerja serta memberikan pelayanan akademik yang baik. Sistem Informasi Akademik (SIKAD) merupakan sistem informasi yang digunakan untuk mengelola data dosen, data mahasiswa serta mengelola pelayanan administrasi akademik seperti Kartu Rencana Studi, Kartu Hasil Studi, input nilai, jadwal dan pembayaran. Hadirnya Sistem Informasi Akademik (SIKAD) sejak tahun 2020 dinilai sangat membantu dosen, pegawai dan mahasiswa dalam melakukan aktivitasnya. Tetapi tidak dapat di pungkiri kemungkinan terjadi ancaman risiko yang terjadi di sistem

dapat mengganggu aktifitas proses bisnis sehingga kegiatan tidak dapat berjalan dengan baik.

Adapun hasil wawancara lainnya yang peneliti lakukan dengan Kepala IT STT Pekanbaru mengenai Sistem Informasi Akademik (SIKAD) dalam penerapannya STT Pekanbaru belum pernah melakukan pengelolaan risiko terhadap SIKAD. Penting dilakukannya suatu analisis manajemen risiko terhadap risiko yang muncul di dalam Teknologi Informasi (TI) tersebut. Sehingga instansi dapat melakukan pencegahan, penanganan, perbaikan terhadap risiko tersebut sesuai tingkat prioritas risiko. Pengelolaan risiko dinilai sebagai tantangan strategis untuk perusahaan dimana mereka akan menghadapi berbagai ancaman yang kompleks [11]. Salah satu pendekatan untuk menguji manajemen risiko teknologi informasi adalah ISO 31000. Standar manajemen risiko ISO 31000 terdiri dari tiga bagian: prinsip, kerangka kerja, dan proses. Pendekatan manajemen risiko didasarkan pada prinsip manajemen risiko [1]. Sistem manajemen risiko yang disiplin dan metodis dapat dibuat dengan menggunakan kerangka kerja sebagai panduan. Proses manajemen risiko adalah tindakan berurutan dan terhubung. ISO 31000:2018 merupakan versi sederhana dari versi 2009. Pada umumnya. Manfaat ISO 31000:2018 adalah dapat mendukung bisnis dalam melakukan manajemen risiko dengan lebih baik. Ini karena standar ini menawarkan panduan, metode, dan prosedur manajemen risiko yang dapat diterapkan pada arsitektur manajemen risiko untuk memastikan implementasi manajemen risiko TI yang lebih efektif[1]. ISO 31000 sangat tepat digunakan karena sudah diakui secara internasional. Mulai dari tahap identifikasi risiko, analisis risiko, sampai evaluasi risiko yang bisa menghasilkan rekomendasi pengelolaan risiko yang sesuai dengan kondisi instansi [12].

Kajian sebelumnya tentang ISO 31000 telah dipublikasikan pada tahun 2017 dengan judul "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS" oleh Stefan Agustinus dkk. Dalam studi ini, membahas tentang bagaimana penilaian aset-aset perusahaan. Dalam analisis ini ditentukan bahwa terdapat dua potensi bahaya dengan tingkat risiko tinggi dan delapan belas potensi risiko dengan tingkat risiko sedang yang dapat mengganggu kinerja perusahaan. Diperkirakan bahwa penilaian risiko akan memungkinkan pengelolaan kerugian perusahaan [13]. Francisca Lady Nice pada tahun 2016 berjudul "Analisis Risiko Teknologi Informasi di Lembaga Penerbangan dan Antariksa Nasional (LAPAN) di situs web SWIFTS menggunakan ISO 31000" yang membahas ISO 31000 secara lebih rinci. Situs web untuk SWIFTS adalah target utama dari penelitian ini. Hasil dari penelitian ini adalah tingkat risiko dari perangkat lunak, perangkat keras, sumber daya manusia, atau elemen prosedural yang terkait dengan sistem SWIFTS, memiliki probabilitas tinggi untuk terjadi dan nilai efek yang signifikan, dengan potensi mengganggu aktifitas operasional bisnis LAPAN sendiri. Oleh karena itu Kepala Divisi IT LAPAN harus melakukan *review* dan menerapkan strategi manajemen risiko yang disarankan [14]. Hasil dari analisis manajemen risiko TI nantinya dapat mempermudah organisasi dalam mengelola risiko yang terjadi.

2. METODOLOGI PENELITIAN

ISO 31000 telah resmi diakui sebagai standar manajemen risiko oleh *International Organization for Standardization* (ISO). Prinsip, kerangka kerja, dan proses manajemen risiko disediakan oleh ISO 31000 dan dapat diterapkan sebagai arsitektur manajemen risiko untuk memastikan bahwa manajemen risiko diterapkan secara efektif. Standar ISO 31000 berlaku untuk bisnis sektor publik dan swasta serta organisasi nirlaba, organisasi komunitas, dan entitas lainnya. Akibatnya, standar ini tidak terpaku pada bisnis atau sektor tertentu [15].

Struktur dan standar yang berlaku universal untuk semua proses manajemen risiko, standar ini dirancang untuk semua jenis bisnis. Karena sifat generik dari manajemen risiko, perlu untuk memasukkan konteks internal dan eksternal ketika menerapkannya, seperti teknologi informasi. Konteks internal mengacu pada pengadaan dan pemeliharaan teknologi dan infrastruktur sistem informasi [16].

Penelitian ini akan dilakukan dengan menggunakan 2 tahapan yang telah disesuaikan dengan proses manajemen risiko dari *International Organization for Standardization* (ISO) di mana setiap informasi yang dibutuhkan dalam penelitian ini didapatkan dengan cara melalui wawancara terhadap sumber-sumber internal dari STT Pekanbaru.

Tahapan pertama adalah penilaian risiko (*Risk Assessment*). Terdiri dari tahap Identifikasi Risiko, Analisis Risiko, dan Evaluasi Risiko. Mengidentifikasi bahaya yang mungkin berdampak pada kemampuan organisasi untuk mencapai tujuannya adalah proses penilaian risiko. Pemahaman yang lebih mendalam tentang risiko dicari melalui analisis risiko. Sedangkan *risk assessment* atau disebut juga penilaian risiko adalah proses penentuan tingkat keseriusan masing-masing risiko berdasarkan kriteria yang telah ditetapkan.

Risk Treatment digunakan untuk tahap kedua. Memilih solusi yang dapat mengurangi atau bahkan sepenuhnya menghilangkan konsekuensi dan potensi bahaya adalah bagian dari tahap ini, yang diikuti dengan mempraktikkan pilihan tersebut.

3. HASIL DAN PEMBAHASAN

Proses manajemen risiko berbasis ISO 31000 meliputi beberapa kegiatan yaitu komunikasi dan konsultasi, penentuan konteks, penilaian risiko, perlakuan risiko, *Monitoring and Review*.

3.1. Komunikasi dan Konsultasi

Membuat rencana komunikasi merupakan langkah awal dalam berinteraksi dengan pihak internal maupun eksternal yang akan berpartisipasi dalam tahapan ini. Setelah itu, dibuat rencana baru mengenai data yang dikumpulkan dan informasi yang akan disampaikan [14].

Wawancara dengan pemangku kepentingan yang terlibat dalam keberlanjutan teknologi dan sistem di STT Pekanbaru dilakukan sebagai bagian dari penelitian dengan menggunakan pendekatan komunikasi langsung. Selain itu juga dilakukan observasi guna memperoleh informasi bagaimana proses bisnis yang diterapkan dalam SIAKAD [17].

3.2. Menetapkan Konteks

Penelitian ini, dilakukan tahapan penetapan konteks. Di mana manajemen risiko, ruang lingkup, dan kriteria risiko akan diperhitungkan. Pihak yang bertanggung jawab, khususnya yang terkait dengan Sistem Informasi Akademik (SIKAD) dan keberlanjutan teknologi, kemudian mengesahkannya. Temuan penetapan konteks manajemen risiko adalah sebagai berikut:

1. Alam atau lingkungan.
2. Manusia.
3. Sistem dan infrastruktur

3.3. Kriteria Risiko

Setelah ditemukan faktor apa saja yang dijadikan konteks risiko yang terjadi, berdasarkan kemungkinan dan dampak maka berikutnya terlebih dahulu disusun kriteria kemungkinan dan kriteria dampak risiko.

Tabel 1. Kriteria Kemungkinan Risiko

Kemungkinan	Toleransi	Kriteria
Sangat Kurang	Tinggi	Rendah
Kurang	Tinggi	Rendah
Sedang	Sedang	Menengah Rendah
Besar	Rendah	Menengah Tinggi
Sangat Besar	Rendah Sekali	Tinggi

Tabel 2. Kriteria Dampak Risiko

Kemungkinan	Toleransi	Kriteria
Sangat Rendah	Tinggi	Rendah
Rendah	Tinggi	Rendah
Sedang	Sedang	Rendah
Besar	Rendah	Menengah Tinggi
Ekstrim	Rendah Sekali	Tinggi

3.4. Penentuan Responden

Berdasarkan RACI Chart, adapun yang menjadi responden kuisisioner ialah orang-orang yang terlibat dalam proses pengelolaan SIKAD.

Tabel 3. RACI Chart

Aktivitas	Peranan		
	Kepala IT	Staff IT	Adm in SIKAD
1. Mengidentifikasi dan mengelola SIKAD	A	C/I	R/I
2. Mengelola, mengoperasikan dan mengevaluasi kegiatan IT	A	C/I	R
3. Memutuskan dan menyetujui serta bertanggung jawab atas pekerjaan staff	R/A	I	C/I
4. Memelihara sistem, jaringan, server dan memberikan rekomendasi untuk perbaikan	A/I	R	C



Berdasarkan RACI Chart diatas maka dapat ditentukan jumlah responden yang akan mendukung penelitian ini adalah sebanyak 3 orang. Adapun rincian responden tersebut adalah Kepala IT, Staff IT dan Admin SIAKAD.

3.5. Penilaian Risiko

Penilaian risiko adalah keseluruhan proses dari identifikasi risiko, analisis risiko dan evaluasi risiko. Penilaian risiko dilakukan secara sistematis, berulang dan kolaboratif berdasarkan pada pengetahuan dan pandangan pemangku kepentingan terhadap risiko.

3.6. Identifikasi Risiko

Tahap identifikasi risiko bertujuan guna mengetahui berbagai kemungkinan risiko yang muncul. Setelah melalui proses studi literatur dan wawancara kepada pihak-pihak terkait dengan Sistem informasi Akademik (SIAKAD) yaitu para pemangku kepentingan dari Sekolah Tinggi Teknologi (STT) Pekanbaru. Tahap ini dilakukan dengan cara mengumpulkan informasi untuk mengetahui risiko apa saja yang memiliki kemungkinan muncul dalam proses bisnis instansi [18].

Dengan berpedoman pada konteks yang telah disetujui pada tahap penetapan konteks. Dalam tahap penetapan konteks sudah ditetapkan ada tiga konteks yang merupakan hal-hal yang menjadi batasan atau tolak ukur internal dan eksternal yang akan dijadikan pertimbangan sumber risiko yaitu; Alam/lingkungan, Manusia, Sistem dan Infrastruktur.

Tabel 4. Daftar Risiko

Kategori Risiko	Risiko	Penyebab	Dampak
Alam atau Lingkungan	Petir	Bencana alam	Koneksi jaringan terganggu
	Kebakaran	Korsleting Listrik	Kerugian bagi perusahaan
Manusia	<i>Human error</i>	Kurangnya pelatihan karyawan baru	Kerugian bagi perusahaan
Sistem dan Infrastruktur	<i>Server down</i>	Listrik padam	Sistem tidak dapat diakses
	<i>Data corrupt</i>	Virus	Data tidak dapat diakses/ditemukan
	Koneksi jaringan tidak stabil	Gangguan pada <i>provider</i> , Listrik padam	Sistem tidak dapat diakses
	Gagal <i>update</i>	<i>Server down</i> , Listrik padam	Data tidak bisa disimpan
	Kerusakan <i>Hardware</i>	Arus listrik tidak stabil	Kerugian terhadap material perusahaan
	<i>Over heat</i>	Cuaca panas	Perangkat panas, Sistem tidak dapat diakses
	Listrik padam	Perbaikan dari PLN	Tidak bisa melakukan aktivitas pada sistem

3.7. Analisis Risiko

Analisis risiko mempunyai tujuan untuk melakukan analisis dampak dan kemungkinan semua risiko yang dapat menunda tercapainya tujuan organisasi, juga semua peluang yang mungkin dihadapi organisasi. Analisis risiko Sistem



Informasi (SIKAD) pada STT Pekanbaru ini meninjau 2 aspek risiko, diantaranya dampak (*impact*) dan kemungkinannya (*probability*).

3.8. Probability Impact Matrix

Matriks kemungkinan dan dampak berisi gabungan dari kemungkinan dan dampak. Dengan menggunakan data dari tabel sebelumnya maka dilakukan dibuatlah grafik risiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak.

Dibawah ini merupakan hasil penilaian kemungkinan dan dampak risiko yang disusun berdasarkan pemahaman dari pihak terkait yaitu 3 orang yang terdiri dari Kepala IT, Staff IT, dan Admin SIKAD.

- N1. Suandi Daulay : Kepala IT
- N2. Ade Fajri : Staff IT
- N3. Mohd Bayu Baheramasyah : Admin

Penilaian dilakukan oleh pihak terkait disajikan dalam bentuk tabel nilai kemungkinan dengan skala 1-5 Setelah didapatkan hasil yaitu faktor apa saja yang menjadi konteks risiko yang terjadi, berdasarkan kemungkinan dan dampak maka selanjutnya disusun terlebih dahulu kriteria kemungkinan dan kriteria dampak risiko.

Tabel 5. Hasil Penilaian Kemungkinan Risiko

No.	Nama Risiko	Nilai Kemungkinan		
		N1	N2	N3
1.	Petir	1	2	1
2.	Kebakaran	1	2	2
3.	<i>Human error</i>	5	3	5
4.	<i>Server down</i>	2	2	2
5.	<i>Data corrupt</i>	3	2	2
6.	Jaringan tidak stabil	4	3	3
7.	<i>Gagal update</i>	2	3	2
8.	Kerusakan <i>Hardware</i>	1	2	2
9.	<i>Over heat</i>	3	2	2
10.	Listrik padam	2	3	3

Tabel 6. Hasil Penilaian Dampak Risiko

No.	Nama Risiko	Nilai Dampak		
		N1	N2	N3
1.	Petir	3	1	5
2.	Kebakaran	5	2	4
3.	<i>Human error</i>	3	3	2
4.	<i>Server down</i>	3	3	2
5.	<i>Data corrupt</i>	3	3	3
6.	Jaringan tidak stabil	4	2	2
7.	<i>Gagal update</i>	2	2	2
8.	Kerusakan <i>Hardware</i>	2	3	2
9.	<i>Over heat</i>	3	3	2
10.	Listrik padam	5	2	2

Kemudian selanjutnya disusun matriks risiko bersumber dari nilai kemungkinan dan dampak risiko tersebut. *Probability Impact Matrix* dibawah ini akan dijadikan dasar dari tingkat keutamaan atau level prioritas penanganan dari risiko yang telah diketahui dengan perhitungan Nilai Prioritas Risiko (RPN). *Risk Priority Number* (RPN) ini sendiri adalah nilai hasil perhitungan menggunakan formula yang telah ditentukan. Nilai Prioritas Risiko (RPN) tersebut dihasilkan dari 2 hasil penilaian komponen risiko yaitu kemungkinan dan dampak.

Tabel 7. Probability Impact Matrix

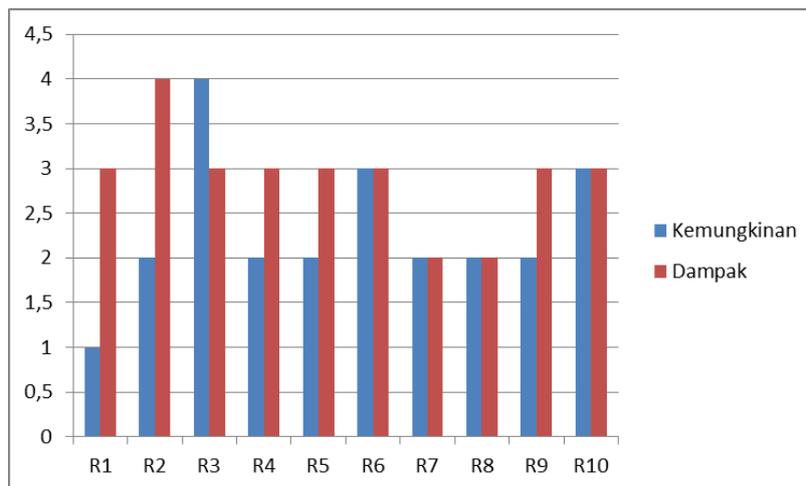
K E M U N G K I N A N	5				
	4			R3	
	3			R6,R10	
	2		R7,R8	R4,R5,R9	R2
	1			R1	
		1	2	3	4

DAMPAK

3.9. Hasil Peringkat Risiko

Hasil Peringkat risiko dibuat berdasarkan Nilai Prioritas Risiko (RPN) menggunakan 2 komponen yaitu kemungkinan terjadinya risiko dan dampak terjadi akibat risiko tersebut yang ditampilkan dalam bentuk matriks kemungkinan dan dampak (*Probability Impact Matrix*).

Adapun grafik risiko dalam konteks risiko pada Sistem Informasi (SIKAD) STT Pekanbaru berdasarkan penilaian dua komponen risiko menurut standard ISO 31000. Grafik risiko berdasarkan sumber risiko dapat dilihat pada Gambar dibawah ini.



Gambar 1. Grafik Risiko

Berikut ini merupakan tabel hasil nilai prioritas risiko (RPN).



Tabel 8. Hasil Nilai Prioritas Risiko (RPN)

No.	Nama Risiko	RPN
1.	Petir	3
2.	Kebakaran	8
3.	<i>Human error</i>	12
4.	<i>Server down</i>	6
5.	<i>Data corrupt</i>	6
6.	Jaringan tidak stabil	9
7.	Gagal <i>update</i>	4
8.	Kerusakan <i>Hardware</i>	4
9.	<i>Over heat</i>	6
10.	Listrik padam	9

3.10. Evaluasi Risiko

Hasil evaluasi risiko akan tampak pada tahapan berikutnya yaitu proses perlakuan risiko. Berdasarkan matriks risiko yang sudah ada, proses evaluasi risiko ini akan berupa tingkatan risiko yang akan dikategorikan menjadi 3 level. Penentuan kategori level of risk ini yaitu kriteria nilai prioritas risiko, yaitu level 1 (*low*), level 2 (*medium*), level 3 (*high*).

Membantu pengambilan keputusan berdasarkan temuan analisis risiko adalah tujuan dari evaluasi risiko. Proses evaluasi risiko akan menentukan risiko mana yang perlu ditangani dan inisiatif apa yang harus diprioritaskan untuk mengatasi risiko tersebut. Hasil dari proses evaluasi risiko ini akan digunakan untuk diolah pada tahap selanjutnya. Adapun tujuan evaluasi risiko adalah untuk memperoleh proses pengambilan penanganan risiko berdasarkan hasil analisis risiko [19].

Tabel 9. Hasil Peringkat Risiko

No.	Kategori	Nama Risiko	RPN	No. Risiko
1.	Level 2 (<i>Medium</i>)	<i>Human error</i>	12	3
2.		Listrik Padam	9	10
3.		Jaringan tidak stabil	9	6
4.		Kebakaran	8	2
5.	Level 1 (<i>Low</i>)	<i>Server down</i>	6	4
6.		<i>Data corrupt</i>	6	5
7.		<i>Over heat</i>	6	9
8.		Gagal <i>update</i>	4	7
9.		Kerusakan <i>hardware</i>	4	8
10.		Petir	3	1

3.11. Perlakuan Risiko

Pada tahap ini tahap ini dimungkinkan untuk melihat langkah-langkah yang diambil untuk risiko yang telah diidentifikasi pada Sistem Informasi Akademik (SIKAD). Menentukan usulan strategi perlakuan risiko yang tepat untuk mengatasi permasalahan yang sesuai dengan pencegahan risiko [20].

Maka usulan perlakuan risiko yang di terapkan ke Sekolah Tinggi Teknologi Pekanbaru antara lain sebagai berikut.

Tabel 10. Usulan Perlakuan Risiko

No.	Risiko	Kategori Risiko	Perlakuan Risiko
1.	<i>Human error</i>	<i>Medium</i>	Memberikan pelatihan sebelumnya jika ada karyawan baru. Membuat <i>knowledge management system</i> sebagai dokumentasi pengetahuan bagi karyawan agar tidak melakukan kesalahan yang sama.
2.	Listrik Padam	<i>Medium</i>	Menyediakan sumber listrik cadangan.
3.	Koneksi jaringan tidak stabil	<i>Medium</i>	Melakukan <i>maintenance</i> jaringan di STT Pekanbaru secara berkala.
4.	Kebakaran	<i>Medium</i>	Memasang server cadangan di lokasi yang berbeda. Membuat <i>database</i> cadangan. Memasang <i>fire hydran</i> di dalam gedung STT Pekanbaru untuk mencegah terjadinya kebakaran.
5.	<i>Server down</i>	<i>Low</i>	Melakukan pengecekan rutin kepada <i>database</i> dari SIAKAD dan <i>database</i> utama STT . Melakukan <i>refresh</i> terhadap penggunaan log, temp, dan RAM dari SIAKAD dan <i>database</i> utama untuk mencegah <i>server down</i> .
6.	<i>Data corrupt</i>	<i>Low</i>	Menjadwalkan <i>backup data</i> . Rutin membersihkan PC secara berkala guna mencegah munculnya virus.
7.	<i>Over heat</i>	<i>Low</i>	Menyediakan pendingin ruangan ataupun pendingin pada perangkat .
8.	Gagal <i>update</i>	<i>Low</i>	Memastikan jaringan stabil ketika melakukan <i>update</i> . Serta hindari <i>traffic jam</i> saat <i>update</i> .
9.	Kerusakan <i>hardware</i>	<i>Low</i>	Membersihkan <i>hardware</i> secara berkala. Segera memberitahukan kepada bagian IT apabila ditemukan gangguan pada perangkat.
10.	Petir	<i>Low</i>	Membuat server cadangan di tempat yang lain. Membuat <i>database cadangan</i> .

3.12. Monitoring and Review

Proses manajemen risiko mencakup *monitoring* dan *review*, yang menjamin setiap tahapan dan fungsi proses berjalan dengan baik. Efektivitas pengendalian risiko yang telah dilakukan sebelumnya tetap berjalan lancar dengan tingkat urgensi yang rendah, tidak terpengaruh, dan pengaruh perubahan keadaan dan lingkungan masih dapat diatur dalam batas-batas *risk appetite*. Dengan kata lain, *monitoring* dan *review* adalah bagian dari proses manajemen risiko yang memastikan bahwa keseluruhan proses manajemen risiko memang berjalan dan mampu memberikan jaminan pencapaian sasaran penerapan manajemen risiko terhadap Sistem Informasi Akademik (SIAKAD) Pada Sekolah Tinggi Teknologi Pekanbaru.

4. SIMPULAN

Berdasarkan analisis yang telah dilakukan, analisis manajemen risiko IT menggunakan ISO 31000 pada sistem informasi akademik (SIKAD) di Sekolah Tinggi Teknologi Pekanbaru. Maka kesimpulan yang di ambil yaitu sebagai berikut:

- a) Mendapatkan nilai *Risk Priority Number* (RPN) yang di dapat dari hasil perkalian Kemungkinan (K) dan Dampak (D) dan mendapatkan nilai tertinggi yaitu *human error*, listrik padam, jaringan tidak stabil dan kebakaran yang masuk dalam kategori *medium* dengan nilai 12, 9, 9, dan 8 secara berurutan. Serta *server down*, *data corrupt*, *over heat*, gagal update, kerusakan *hardware* dan petir dalam kategori *Low* dengan nilai 6, 6, 6, 4, 4, dan 3 secara berurutan.
- b) Mendapatkan rekomendasi perlakuan risiko-risiko yang terletak di prioritas risiko, sebagai acuan dan bahan pengambilan keputusan atau perbaikan atas risiko di Sistem Informasi Akademik (SIKAD). Seperti Human error yang merupakan risiko tertinggi mendapat perlakuan risiko dengan cara memberikan pelatihan sebelumnya jika ada karyawan baru. Serta membuat *knowledge management system* sebagai dokumentasi pengetahuan bagi karyawan agar tidak melakukan kesalahan yang sama.

DAFTAR PUSTAKA

- [1] Mahardika, Krisdana Bima, Agustinus Fritz Wijaya dan Ariya Dwika Cahyono. 2019. "Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000:2018 (Studi Kasus: CV. XY)." *Sebatik* 23(1):277-84. doi: 10.46984/sebatikv23i1.572.
- [2] Grey, Manson, S., & Louise, C. (2015). *The Audit Process: Principles, Practice and Cases, 6th edition*. Cengage Learning
- [3] Angraini, A., dan Pertiwi, I. D. (2017). Analisa pengelolaan risiko penerapan teknologi informasi menggunakan iso 31000. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, 3(2), 70-76.
- [4] Nurbaya, F., Witanti, W., dan Umbara, F. R. (2017). Manajemen risiko sistem informasi akademik di universitas jenderal achmad yani menggunakan committee of sponsoring organizations of the treadway commission's (coso). *Prosiding SNST Fakultas Teknik*, 1(1).
- [5] A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus: iGracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study: iGracias Telkom University)," *e-Proceeding Eng.*, vol. 2, no. 2, pp. 6201-6208, 2015.
- [6] Harimurti, F., 2006, Manajemen Risiko, Fungsi dan Mekanismenya, *Jurnal Ekonomi dan Kewirausahaan*, no. 1, vol. 6, hal 105-112.
- [7] Iswajuni, I., Manasika, A., & Soetedjo, S. (2018). The effect of enterprise risk management(ERM) on firm value in manufacturing companies listed on Indonesian Stock Exchange year 2010-2013. *Asian Journal of Accounting Research*, 3(2):224-235.
- [8] Aisyah, A. P., dan Dahlia, L. (2022). Enterprise risk management berdasarkan ISO 31000 dalam pengukuran Risiko Operasional Pada Klinik spesialis esti. *Jurnal Akuntansi Dan Manajemen*, 19(02), 78-90. <https://doi.org/10.36406/jam.v19i02.483>.
- [9] Vorst, Charles R, D., Priyarsono, dan Arif Budiman. 2018. MANAJEMEN RISIKO BERBASIS SNI ISO 31000.
- [10] Manoppo, Franky. 2017. "Perencanaan Strategis Sistem Informasi Menggunakan Metode *Ward and Peppard* Pada PT. Serasi Autoraya." *Sebatik* 23(1):185-91. doi: 10.46984/sebatikv23i1.467.
- [11] C. Lalonde and O. Boiral, "Managing risks through ISO 31000: A critical analysis," *Risk Manag.*, vol. 14, no. 4, pp. 272-300, Nov. 2012.



- [12] P. P. Thenu, A. F. Wijaya, and C. Rudianto, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus: Pt Global Infotech)," *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13, 202.
- [13] Agustinus, S., Nugroho, A., & Cahyono, A. D. (2017). Analisis Risiko Teknologi informasi menggunakan ISO 31000 PADA program HRMS. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 1(3), 250–258. <https://doi.org/10.29207/resti.v1i3.94>.
- [14] Nice, Francisca Lady, dan Radiant Victor Imbar. 2016. "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000." *Jurnal Informatika dan Sistem Informasi* 2(2):1689–99.
- [15] Susilo, L. dan Kaho, R. (2018). *Manajemen risiko berbasis iso 31000: untuk industri nonperbankan*. edisi revisi. Jakarta: PPM.
- [16] Fernando, Andri. 2020. "Analisis Manajemen Risiko Sistem Informasi *Automotive Management System* (AMS) Menggunakan Metode ISO 31000".
- [17] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.
- [18] D. E. Adi and N. Susanto, "Analisis Manajemen Risiko Aktivitas Pengadaan pada Percetakan Surat Kabar," *J. Metris*, vol. 18, pp. 113–118, 2017.
- [19] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM (Jurnal Riset Komputer)*, vol. 7, no. 1, p. 9.
- [20] A. R. Tampubolon and Suhardi, "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 : 2009 Studi Kasus : Pembobolan ATM BCA Tahun 2010," *J. Telemat.*, vol. 7, no. 2, pp. 1–10, 2011.