Buletin Sistem Informasi dan Teknologi Islam
Vol 4, No 1, February 2023, pp. 51-58
ISSN: 2721-0901

Analisis Risiko Sistem Informasi Menggunakan ISO 31000 Sebagai Upaya Manajemen Risiko

Syahrul[a,1,*], Ramdan Satra[a,2], Farniwati Fattah[a,3],

[a] *Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Jl. Urip Sumoharjo KM.05, Makassar 90231, Indonesia*
[1] *syahrul.yf@gmail.com;* [2] *ramdan.satra@umi.ac.id;* [3] *farniwati.fattah@umi.ac.id*
**corresponding author*

INFORMASI ARTIKEL

Diterima : 07-02-2023
Direvisi : 21-02-2023
Diterbitkan : 28-02-2023

Kata Kunci:
Sistem Informasi
ISO 31000:2018
Manajemen Risiko

ABSTRAK

Sistem informasi studio.fikom.umi.ac.id adalah unit yang dikelola oleh Fakultas Ilmu Komputer Universitas Muslim Indonesia. Unit ini dibentuk sebagai lembaga pelatihan dan ujian sertifikasi bagi Dosen, Karyawan, Mahasiswa, Praktisi dalam lingkup UMI atau umum. Sistem informasi memiliki risiko yang beragam yang disebabkan oleh beberapa faktor misalnya alam/lingkungan, manusia serta sistem dan infrastruktur. Berdasarkan permasalahan tersebut, maka dilakukan penelitian untuk mendokumentasikan berbagai macam kemungkinan risiko serta prioritas risiko-risiko yang dapat mengganggu jalannya sistem informasi studio.fikom.umi.ac.id. penelitian ini menggunakan ISO 31000:2018. ISO 31000 merupakan standar pengelolaan risiko yang terdiri atas tiga elemen yakni: prinsip (*principle*), kerangka kerja (*framework*), dan proses (*process*). Hasil penelitian menunjukkan 30 kemungkinan risiko yang berpotensi mengganggu kinerja studio.fikom.umi.ac.id. Terdapat 6 kemungkinan risiko yang masuk ke dalam *level of risk* tingkatan *high*. Berikutnya ada 18 kemungkinan risiko yang masuk ke dalam *level of risk* tingkatan *medium*. Serta terdapat 6 kemungkinan risiko yang masuk ke dalam *level of risk* tingkatan *low*.

I. Pendahuluan

Fakultas Ilmu Komputer memiliki beberapa sistem informasi yakni: fikom.umi.ac.id, siakad.umi.ac.id, apps.fikom.umi.ac.id dan studio.fikom.umi.ac.id. Salah satu diantara sistem informasi tersebut adalah studio.fikom.umi.ac.id. Sistem informasi ini adalah unit yang dikelola oleh Fakultas Ilmu Komputer UMI (Universitas Muslim Indonesia). Unit ini dibentuk sebagai lembaga pelatihan dan ujian sertifikasi bagi Dosen, Karyawan, Mahasiswa, Praktisi dalam lingkup UMI atau umum. Dalam penerapan sistem informasi pasti memiliki berbagai kemungkinan risiko yang dapat mengganggu, sehingga sistem informasi yang dijalankan tidak berjalan secara optimal [1]. Tidak terkecuali studio.fikom.umi.ac.id dapat mengalami kemungkinan-kemungkinan yang muncul disekitarnya. Sistem informasi memiliki risiko yang beragam seperti kebocoran data karena hacker, kerusakan sistem akibat terkena virus, *human error*, kebakaran, kegagalan kelistrikan karena faktor alam dan lainnya [2] Berdasarkan permasalahan tersebut, maka dibutuhkan penelitian untuk mendokumentasikan berbagai macam kemungkinan risiko serta prioritas risiko-risiko tersebut terhadap sistem informasi studio.fikom.umi.ac.id. Sehingga dengan tujuan tersebut dapat dilakukan analisis manajemen risiko menggunakan ISO 31000 [3].

Adapun penelitian terkait mengenai penelitian ini. Pertama, penelitian yang dilakukan Krisdana Bima Mahardika, Agustinus Fritz Wijaya, dan Ariya Dwika Cahyono. Hasil penelitian ini didapatkan hasil bahwa ada 5 kemungkinan risiko dengan tingkatan low, 18 kemungkinan risiko dengan tingkatan medium, dan 2 kemungkinan risiko dengan tingkatan high [4]. Melakukan manajemen risiko teknologi informasi pada CV.XY menggunakan ISO 31000:2018. Kemudian penelitian yang dilakukan Dewangga Lazuardi Ramadhan, Ronie Febriansah, Renny Sari Dewi. Dari hasil analisis yang diperoleh dari proses evaluasi risiko menggunakan tabel matriks, bahwa nilai risiko ekstrim ada 1, risiko tinggi ada 2, untuk risiko sedang ada 4 dan untuk risiko rendah ada 5 [5].

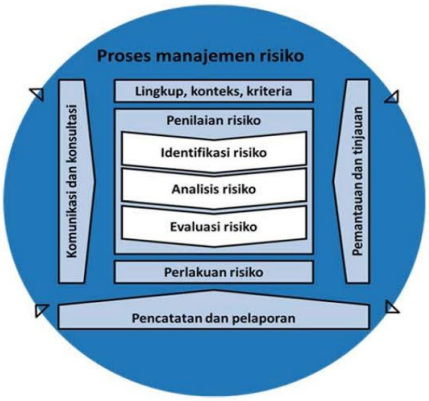
Pada penelitian terdahulu menggunakan ISO 31000 versi 2009 dan hasil penelitiannya sampai pada tahap mengetahui risiko, dampak risiko serta level risiko, pada penelitian ini dilakukan pengembangan sampai pada tahap rekomendasi terhadap perlakuan risiko. Pada penelitian ini akan dilakukan analisis manajemen risiko

pada sistem informasi studio.fikom.umi.ac.id untuk mengidentifikasi kemungkinan risiko yang dapat mengganggu, selanjutnya mengidentifikasi dampak yang diakibatkan risiko tersebut, kemudian melakukan penilaian dan evaluasi risiko serta tindakan yang akan dilakukan untuk mengantisipasi risiko tersebut [3]. Hasil analisa diharapkan dapat digunakan studio.fikom.umi.ac.id. dalam menyusun kebijakan untuk meminimalisir kemungkinan-kemungkinan risiko yang akan muncul dan mengganggu jalanya studio.fikom.umi.ac.id di kemudian hari.

II. Metode

A. ISO 31000:2018

ISO 31000 merupakan standar pengelolaan risiko yang terdiri atas tiga elemen: prinsip (*principle*), kerangka kerja (*framework*), dan proses (*process*). Standar ini ditujukan untuk dapat diterapkan dan disesuaikan untuk semua jenis organisasi dengan memberikan struktur dan pedoman yang berlaku generik terhadap semua operasi yang terkait dengan manajemen risiko [3].



Gambar 1. Proses Manajemen Risiko [6]

Proses manajemen risiko terdiri 2 tahap yaitu, *risk assessment* dan *risk treatment* [7], pertama *risk assessment*, terdiri dari beberapa tahap berikut:

1) Identifikasi Risiko (Risk Identification)

Usaha dalam mengumpulkan informasi guna mendapatkan risiko–risiko apa saja yang kemungkinan muncul dalam kegiatan–kegiatan operasional yang dikerjakan oleh studio.fikom.umi.ac.id [8].

2) Analisis Risiko (Risk Analysis)

Tahap ini dilakukan proses analisis risiko dengan menentukan nilai dari kemungkinan-kemungkinan risiko yang telah diidentifikasi pada tahap sebelumnya. Pada proses ini menggunakan tabel kriteria *likelihood* yang dibedakan menjadi lima kriteria dari berapa banyaknya kemungkinan risiko yang terjadi dalam kurun waktu tertentu [8].

Tabel 1. Nilai Kriteria Likelihood Model

Likelihood		**Deskripsi**	**Frekuensi Kejadian**
Nilai	**Kriteria**		
1.	*Rare*	Risiko sangat jarang terjadi	>2 tahun
2.	*Unlikely*	Risiko jarang terjadi	1-2 tahun
3.	*Possible*	Risiko cukup sering terjadi	7-12 bulan
4.	*Likely*	Risiko sering terjadi	4-6 bulan
5.	*Certain*	Risiko selalu terjadi	1-6 bulan

Kemudian dilakukan tahap penilaian dari dampak yang terjadi pada objek kasus terhadap kemungkinan risiko yang terjadi [8].

Tabel 2. Nilai Kriteria *Impact*

Impact		**Deskripsi**
Nilai	**Kriteria**	
1	*Insignificant*	Risiko tidak mengganggu aktivitas dan proses bisnis pada instansi.
2	*Minor*	Aktivitas pada instansi sedikit terhambat, namun tidak mengganggu aktivitas inti pada instansi.
3	*Moderate*	Risiko tersebut mengganggu jalannya proses bisnis pada instansi, sehingga aktivitas bisnis sedikit terhambat.
4	*Major*	Risiko tersebut menghambat hampir seluruh jalannya proses bisnis pada instansi.
5	*Catastrophic*	Risiko mengganggu jalannya proses bisnis yang ada secara menyeluruh dan menghentikan aktivitas instansi secara total.

3) Evaluasi Risiko (Risk Evaluation)

Tujuan dari evaluasi risiko ini adalah untuk mendapatkan proses pengambilan risiko berdasarkan hasil analisis risiko. Hingga kemudian menghasilkan analisis risiko untuk dapat dikategorikan sebagai 3 level risiko yaitu: *low*, *medium*, dan *high* [8].

Tabel 3. Matriks Evaluasi Risiko

Likelihood	***Certain***	**5**	*Medium*	*Medium*	*High*	*High*	*High*
	Likely	**4**	*Medium*	*Medium*	*Medium*	*High*	*High*
	Possible	**3**	*Low*	*Medium*	*Medium*	*Medium*	*High*
	Unlikely	**2**	*Low*	*Low*	*Medium*	*Medium*	*Medium*
	Rare	**1**	*Low*	*Low*	*Low*	*Medium*	*Medium*
	Impact		**1**	**2**	**3**	**4**	**5**
			Insignificant	***Minor***	***Moderate***	***Major***	***Catastrophic***

Keterangan risiko:

High Risk : Risiko yang berbahaya yang harus diatasi secepatnya

Medium Risk : Risiko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan

Low Risk : Risiko ini dapat diabaikan dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh paling kecil

Tahap kedua adalah *Risk Treatment* akan mencantumkan satu atau lebih pilihan untuk menanggulangi risiko sehingga dapat menerapkan penanganan risiko [8]. Secara umum perlakuan terhadap suatu risiko dapat berupa salah satu dari keempat perlakuan sebagai berikut: pencegahan risiko (*Risk Prevention*), berbagi risiko (*Risk Sharing/Transfer*), mitigasi (*Mitigation*), retensi risiko (*Risk Retention*) [10].

III.Hasil dan Pembahasan

A. Penilaian Risiko (Risk Assessment)

1) Identifikasi Risiko (risk identification)

a. Identifikasi Aset

Tahapan identifikasi aset pada sistem informasi studio.fikom.umi.ac.id dilaksanakan melalui beberapa proses diantaranya: wawancara, observasi, dan studi pustaka. Detail aset-aset terkait dapat dilihat pada tabel berikut.

Tabel 4. Identifikasi Aset studio.fikom.umi.ac.id

No. Aset	Komponen SI/TI	Aset	Lokasi
A1	Data	Data Pendaftaran Peserta Ujian	studio.fikom.umi.ac.id
A2		Data Transaksi Pembayaran	studio.fikom.umi.ac.id
A3		Data Pengguna	studio.fikom.umi.ac.id
A4	*Software*	Aplikasi Compass	*PC* Studio Informatika
A5	*Hardware*	Komputer	Ruang Studio Informatika
A6		*Keyboard*	Ruang Studio Informatika
A7		*Mouse*	Ruang Studio Informatika
A8		*CPU*	Ruang Studio Informatika
A9		*Wi-fi*	Ruang Studio Informatika

2) Identifikasi Kemungkinan Risiko, Dampak Risiko dan Analisis Risiko (Risk Analysis)

Tahap ini dilakukan identifikasi kemungkinan risiko yang dapat terjadi. Selanjutnya dilakukan identifikasi dampak risiko yang akan dialami oleh studio.fikom.umi.ac.id jika kemungkinan-kemungkinan yang sudah diidentifikasi sebelumnya terjadi.

Kemudian dilakukan penilaian terhadap kemungkinan risiko yang telah diidentifikasi. Penentuan nilai berdasarkan kemungkinan (*likelihood*) pada tabel 1 dan dampak (*impact*) pada tabel 2. Frekuensi dan dampak diisi dengan angka 1 sampai dengan 5 sesuai dengan kondisi yang ada.

Tabel 5. Kemungkinan Risiko, Dampak Risiko, Analisis Risiko

Nomor Ancaman	Faktor	Kemungkinan Risiko	Dampak Risiko	Likelihood	Impact
KR1	Alam/Lingkungan	Kebakaran	Kerusakan Infrastruktur, Kerugian Finansial, menghentikan aktivitas studio.fikom.umi.ac.id.	1	5
KR2	Alam/Lingkungan	Gempa Bumi	Kerusakan Infrastruktur, Kerugian Materil, Menghentikan aktivitas studio.fikom.umi.ac.id.	1	5
KR3	Alam/Lingkungan	Petir	Kerusakan infrastruktur studio.fikom.umi.ac.id.	1	1
KR4	Alam/Lingkungan	Debu Dan Kotoran	Alat mengalami kerusakan	5	1
KR5	Alam/Lingkungan	Listrik Padam	Kerugian operasional studio.fikom.umi.ac.id, Mengganggu proses kerja *server*, Kualitas *server* menurun.	5	2
KR6	Manusia	Penyalahgunaan Hak Akses	Bocornya data, Manipulasi data.	1	4
KR7	Manusia	*Human Error*	Proses layanan tidak berjalan dengan optimal, Mengganggu proses studio.fikom.umi.ac.id.	1	4
KR8	Manusia	*User Interface* Sulit Dipahami	*User* sulit memahami cara penggunaan sistem informasi, Memperlambat proses kerja.	2	2
KR9	Manusia	Pencurian Perangkat	Kerugian secara finansial, Proses studio.fikom.umi.ac.id terganggu.	1	3

KR10	Manusia	Kerusakan Akibat Manusia *(Cybercrime)*	Kerusakan *hardware* ataupun perangkat lainnya .	1	2
KR11	Manusia	Pengunduran Diri	Sulit mencari pengganti staff yang ahli dan berpengalaman di bidang pekerjaan, Proses studio.fikom.umi.ac.id terganggu.	2	3
KR12	Manusia	Pegawai Yang Sakit	Sulit mencari pengganti staff yang ahli dan berpengalaman di bidang pekerjaan.	5	4
KR13	Manusia	Petugas Tidak Mengikuti SOP	Alat rusak, Kerja tidak optimal.	4	3
KR14	Manusia	Peretasan *Database*	Merusak sistem, Memanipulasi data, Mencuri data.	3	4
KR15	Manusia	Kelalaian *Maintenance* Hardware Secara Berkala	Tidak dapat mendeteksi kerusakan *hardware.*	4	5
KR16	Manusia	Teknologi Yang Digunakan Tidak *Update*	Proses kerja melambat, studio.fikom.umi.ac.id, menjadi sulit untuk berkembang dan tidak mengikuti tren.	2	3
KR17	Sistem dan Infrastruktur	*Server Down*	studio.fikom.umi.ac.id tidak dapat diakses, Menghambat proses studio.fikom.umi.ac.id.	3	4
KR18	Sistem dan Infrastruktur	*Overload*	Kehilangan data, Lambat *loading*	2	4
KR19	Sistem dan Infrastruktur	*Overheat*	Kinerja *hardware* kurang maksimal, karena rusaknya *hardware* yang harus menanggung suhu panas yang terus menerus, *Software* yang sedang digunakan menjadi lambat/*error*, Proses studio.fikom.umi.ac.id terganggu.	2	4
KR20	Sistem dan Infrastruktur	Koneksi Jaringan Terputus	Gagal *update* data, Kehilangan data, Proses studio.fikom.umi.ac.id terganggu.	4	5
KR21	Sistem dan Infrastruktur	*Web Service* Mati Secara Tiba-Tiba	Tidak dapat mengakses studio.fikom.umi.ac.id, Kemungkinan hilangnya data, Proses studio.fikom.umi.ac.id terganggu.	1	5
KR22	Sistem dan Infrastruktur	*Data Corrupt*	studio.fikom.umi.ac.id tidak dapat menerima data yang valid, Data rusak, Dapat mengalami kehilangan data.	2	5

KR23	Sistem dan Infrastruktur	*Backup Failure*	studio.fikom.umi.ac.id tidak memiliki data cadangan, Meningkatkan risiko kehilangan data.	1	5
KR24	Sistem dan Infrastruktur	Proses *Maintenance* Tidak Terjadwal	Menyebabkan sering terjadinya *error* pada studio.fikom.umi.ac.id.	4	5
KR25	Sistem dan Infrastruktur	Serangan *Virus*	Kehilangan data ,Proses studio.fikom.umi.ac.id terganggu, Data *corrupt.*	5	4
KR26	Sistem dan Infrastruktur	Kegagalan *Software*	Kehilangan data, Proses studio.fikom.umi.ac.id sangat terganggu, Kerugian secara finansial.	3	4
KR27	Sistem dan Infrastruktur	Kegagalan *Hardware*	Kehilangan data, Proses studio.fikom.umi.ac.id sangat terganggu, Kerugian secara finansial.	2	4
KR28	Sistem dan Infrastruktur	*Overcapacity*	Kapasitas memori penuh sehingga *database* tidak dapat menampung data berlebih.	1	3
KR29	Sistem dan Infrastruktur	Sistem *Crash*	Kerusakan sistem yang menyebabkan, studio.fikom.umi.ac.id tidak dapat diakses dalam jangka waktu sementara.	1	3
KR30	Sistem dan Infrastruktur	Gagal *Update*	User tidak dapat menggunakan fitur terbaru, Rentan mengalami peretasan.	2	3

3) Evaluasi risiko (risk evaluation).

Pada tahap ini menggunakan acuan berupa matriks risiko, penentuan matriks dapat dilihat pada tabel 3. Setelah kemungkinan-kemungkinan risiko dimasukan ke dalam matriks evaluasi berdasarkan *likelihood* dan *impact*. Maka didapatkan 6 kemungkinan risiko yang masuk ke dalam *level of risk* tingkatan *high*, 18 kemungkinan risiko yang masuk ke dalam *level of risk* tingkatan *medium*, dan 6 kemungkinan risiko yang masuk ke dalam *level of risk* tingkatan *low*.

B. Perlakuan Risiko (Risk Treatment)

Pada tahap ini akan di berikan usulan-usulan yang dapat digunakan untuk memperlakukan kemungkinan-kemungkinan risiko tersebut

Tabel 6. Usulan Perlakuan Risiko

Nomor Ancaman	**Kemungkinan Risiko**	***Risk Level***	***Risk Treatment***
KR5	Listrik Padam	*High*	Menyediakan generator set listrik dengan daya yang sesuai dengan kebutuhan. Kemudian menyiapkan *Uninterruptible Power Supply (UPS).*
KR12	Pegawai Yang Sakit	*High*	Pegawai/karyawan yang bekerja dibuat dengan sistem shift, sehingga jika ada pegawai sakit maka akan digantikan pegawai lain, Melakukan pelatihan terhadap karyawan.
KR15	Kelalaian *Maintenance Hardware* Secara Berkala	*High*	Membuat jadwal *maintenance hardware* secara berkala, supaya teknisi dapat memperkirakan *hardware* mana yang perlu diganti atau diperbaiki.

KR20	Koneksi Jaringan Terputus	*High*	Memasang 2 *internet service provider / ISP*, sehingga ketika 1 *provider* mengalami gangguan maka *provider* yang lain bisa segera digunakan dan melapor ke pihak *ISP*.
KR24	Proses *Maintenance* Tidak Terjadwal	*High*	Melakukan penjadwalan *maintenance* rutin.
KR25	Serangan *Virus*	*High*	Melakukan *scanning* anti virus terhadap *portable device*, serta selalu mengaktifkan *firewall* dan internet *security*.
KR1	Kebakaran	*Medium*	Menyiapkan alat pemadam kebakaran disekitar area studio.fikom.umi.ac.id.
KR2	Gempa Bumi	*Medium*	Menyediakan tempat yang aman untuk semua perangkat.
KR4	Debu Dan Kotoran	*Medium*	Melakukan perawatan kebersihan untuk meminimalisir risiko kerusakan.
KR6	Penyalahgunaan Hak Akses Oleh Karyawan	*Medium*	Memberikan batasan akses pada setiap *user*, Memasang dan memantau *CCTV* di gedung instansi dan ruangan studio.fikom.umi.ac.id.
KR7	Human Error (Kesalahan Yang Dilakukan Karyawan)	*Medium*	Melakukan pelatihan terhadap karyawan dan melakukan pemetaan kemampuan masing-masing individu, Melakukan pembagian tugas sesuai dengan kemampuan masing-masing individu, Membuat dan menjalankan SOP agar tahu lebih jelas peraturan di bidang kerjanya.
KR11	Pengunduran Diri	*Medium*	Untuk mencegah pegawai melakukan pengunduran diri, diperlukannya pemetaan terhadap kemampuan dan melakukan pembagian tugas sesuai dengan kemampuan.
KR13	Petugas Tidak Mengikuti SOP	*Medium*	Membuat dokumen SOP untuk setiap bidang pekerjaan supaya lebih jelas aturannya.
KR14	Peretasan *Database*	*Medium*	Memasang antivirus yang mumpuni dan selalu melakukan *update*.
KR16	Teknologi Yang Digunakan Tidak *Update*	*Medium*	Mengganti/memperbaharui *hardware dan software* dengan yang lebih baru sehingga kinerja sistem bisa lebih baik.
KR17	*Server Down*	*Medium*	Melakukan pemeriksaan berkala pada *database*.
KR18	*Overload*	*Medium*	Melakukan *monitoring* berkala dan melakukan *backup* data secara berkala.
KR19	*Overheat*	*Medium*	Menyediakan ruang yang memiliki *AC* (*Air Conditioner*) dan menambah *fan* pada semua *hardware* yang membutuhkan.
KR21	*Web Service* Mati Secara Tiba-Tiba	*Medium*	Memberikan pemberitahuan kepada *user* saat *web service* mati, Melakukan *troubleshooting* saat *web service* mati.
KR22	*Data Corrupt*	*Medium*	Memproteksi *PC* dengan antivirus secara berkala untuk mencegah munculnya *virus/malware*, Melakukan *backup* data secara berkala.
KR23	*Backup Failure*	*Medium*	Memperhatikan penggunaan memori yang digunakan *database* agar jangan sampai penuh. Membuat *maintenance* plan yang tepat. Serta membuat SOP dan melakukan backup data secara berkala.
KR26	Kegagalan *Software*	*Medium*	Melakukan pengecekan terhadap *driver*, *IRQ*, atau *resource* lainya pada *PC*, jika diperlukan melakukan install ulang pada *OS*.
KR27	Kegagalan *Hardware*	*Medium*	Memberikan asuransi terhadap aset *hardware* yang ada.
KR30	Gagal *Update*	*Medium*	Memastikan kualitas jaringan sebelum melakukan *update*.
KR3	Petir	*Low*	Memasang alat penangkal petir, Menyiapkan cadangan dan penggantian perangkat jika terjadi risiko petir.
KR8	*User Interface* Sulit Dipahami	*Low*	Membuat tutorial cara menggunakan studio.fikom.umi.ac.id, diunggah ke internet, Memperbaharui *UI* agar lebih sederhana.
KR9	Pencurian Perangkat Keras	*Low*	Memperbanyak titik-titik pemasangan *CCTV* diarea studio.fikom.umi.ac.id, Melakukan penjagaan yang ketat terhadap *hardware*.
KR10	*Vandalisme*	*Low*	Memasang dan memantau *CCTV* di area studio.fikom.umi.ac.id.
KR28	*Overcapacity*	*Low*	Menambah kapasitas memori yang lebih besar agar daya tampungnya lebih optimal. Melakukan cek memori secara berkala.
KR29	*Sistem Crash*	*Low*	Membuat jadwal maintenance dan melakukan back up data secara berkala.

IV. Kesimpulan dan saran

Dari hasil analisis risiko yang sudah dilakukan didapatkan 30 kemungkinan risiko yang berpotensi mengganggu kinerja studio.fikom.umi.ac.id. Terdapat 6 kemungkinan risiko yang masuk ke dalam level of risk tingkatan high. Berikutnya ada 18 kemungkinan risiko yang masuk ke dalam level of risk tingkatan medium. Serta terdapat 6 kemungkinan risiko yang masuk ke dalam level of risk tingkatan low. Dengan melihat situasi di studio.fikom.umi.ac.id dalam mengatasi risiko, belum memiliki pedoman dalam melakukan manajemen risiko sehingga proses penanggulangan risiko secara berkala belum dilakukan secara optimal, maka hasil dari penelitian ini diharapkan dapat digunakan studio.fikom.umi.ac.id. dalam menyusun kebijakan untuk meminimalisir kemungkinan-kemungkinan risiko yang akan muncul dan mengganggu jalannya sistem informasi di kemudian hari.

Untuk penelitian kedepannya diharapkan penulis dapat mengembangkan lagi penelitian ini dengan metode yang lebih relevan atau dapat menggabungkan 2 metode, karena kemungkinan studio.fikom.umi.ac.id. akan terus berkembang. Untuk penelitian kedepannya diharapkan penulis dapat mengembangkan lagi penelitian ini dengan menambahkan poin-poin pertanyaan untuk mendapatkan hasil penelitian yang lebih akurat.

Daftar Pustaka

[1] F. M. Hutabarat and A. D. Manuputty, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional menggunakan ISO 31000," *J. Bina Komput.*, vol. 2, no. 1, pp. 52–65, 2020.

[2] 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," *J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 20, no. 2, pp. 389–396, 2021, doi: 10.30812/matrik.v20i2.1093.

[3] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Pada Aplikasi SAP di PT Serasi Autoraya menggunakan ISO 31000," *Sebatik*, vol. 23, no. 1, pp. 36–43, 2019, doi: 10.46984/sebatik.v23i1.441.

[4] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi menggunakan ISO 31000 : 2018 (Studi Kasus: CV. XY)," *Sebatik*, pp. 277–284, 2018.

[5] D. L. Ramadhan and R. S. D. Ronie Febriansah, "Analisis Manajemen Risiko menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, pp. 91–96, 2020, doi: 10.30865/jurikom.v7i1.1791.

[6] S. SUTIONO, "ISO 31000: Pengertian, Fungsi dan Prinsip," *DosenIT.com*, 2020. https://dosenit.com/ilmu-komputer/iso-31000 (accessed Jun. 24, 2022).

[7] H. C. Christian and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi pada BANK ABC menggunakan Framework ISO 31000," *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 1, pp. 735–748, 2022.

[8] W. Harefa and K. D. Hartomo, "Analisis Manajemen Risiko dengan menggunakan Framework ISO 31000:2018 pada Sistem Informasi Gudang," *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 1, pp. 407–420, 2022.

[9] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo menggunakan ISO 31000," *JCSE (Journal Comput. Sci. an Eng.*, vol. 1, no. 2, pp. 129–145, 2020.

[10] O. D. Pebriani and D. H. Zulfikar, "Analisis Manajemen Risiko Teknologi Informasi menggunakan ISO 31000 Pada Website SIMPEG di Kantor Kementerian Agama Kota Palembang," in *SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika*, 2022, pp. 183–190.