Jurnal Bina Komputer
JBK, Vol. 2, No. 2, Juli 2020: 1-14
Received: 15 Maret 2020; Revised: 27 April 2019; Accepted: 30 Juni 2020

Analisis Manajemen Risiko Aplikasi SINTESA Pada Perpustakaan XYZ

Rifky Prima Pangestu[1], Agustinus Fritz Wijaya[2]

Program Studi Sistem Informasi
Universitas Kristen Satya wacana
email :[1,2] 682017013@student.uksw.edu, agustinus.wijaya@uksw.edu
Jl. DiPonegoro No. 52-60, Salatiga

Abstract

The Sintesa application is an operation support information system application that functions to assist the XYZ Library in recording loan books, a list of available books, the number of books, book loan maturities, and a list of book borrowers. In implementing this information system, there are certain risks that will hinder the process or function of the system, so a risk analysis is needed to prevent the risks that will occur. By using ISO 31000 in the XYZ library, it is hoped that it can minimize the possible risks that will occur around the SINTESA application. The results of the risk analysis with ISO 31000 in the form of documentation of possible risks that exist around the SINTESA application, classifying the possibilities - risks based on their impact. So that the results of this risk analysis can be used by the library to prevent and minimize risks and treat these risks according to the impact or risk priority that may occur in the library application.
Keyword**:** *ISO 31000, Application SINTESA, Risk Management.*

Abstrak

Aplikasi Sintesa merupakan aplikasi sistem informasi operasi pendukung yang berfungsi untuk membantu Perpustakaan XYZ dalam mencatat buku pinjaman, daftar buku yang tersedia, jumlah buku, jatuh tempo peminjaman buku, dan daftar peminjam buku. Dalam implementasi sistem informasi ini pasti terdapat risiko risiko yang akan menghambat proses atau fungsi dari sistem tersebut, maka dibutuhkan analisis risiko untuk mencegah risiko - risiko yang akan terjadi. Dengan menggunakan ISO 31000 di perpustakan XYZ ini di harapkan dapat menimalisir kemungkinan – kemungkinan risiko yang akan terjadi di sekitar aplikasi SINTESA. Hasil dari analisis risiko dengan ISO 31000 berupa dokumentasi kemungkinan risiko yang ada disekitar aplikasi SINTESA, mengelompokkan kemungkinan – kemungkinan risiko yang berdasarkan dampaknya. Sehingga hasil dari analisis risiko ini dapat di gunakan perpustakaan untuk mencegah dan meminimalisir risiko serta memperlakukan risiko tersebut sesuai dampak atau prioritas risiko yang kemungkinan terjadi di aplikasi perpustakaan tersebut.
Kata kunci: ISO 31000, Aplikasi SINTESA, Manajemen Risiko.

1. PENDAHULUAN

Di zaman modern ini perkembangan teknologi sangat berkembang sangat pesat dan hampir dari seluruh aspek kehidupan sangat bergantung dengan yang namanya teknologi, seperti: media sosial (tempat berkomunikasi online), e-commerce (pasar online) e-commerce ini juga sangat berdampak baik disaat sekarang yang dimana dunia sedang di landa pandemic virus, serta tidak lupa e-book (perpustakaan online) dan masih banyak hal lainnya lagi. Perpustakaan yang dulunya semua aktivitas bisnisnya seperti peminjaman buku, pengembalian buku, pembayaran denda, dan lain-lain masih dilakukan secara offline dan yang sebenarnya tidak efisien, dengan munculnya teknologi di era sekarang sangat berdampak positif bagi perpustakan yang bertujuan mempercepat dan mempermudah menjalankan aktivitas bisnisnya.

Setiap hal didunia ini pasti mempunyai dampak negatif dan positifnya, seperti halnya dengan teknologi dilain sisi mempermudah aktivitas kita, dan dilain sisi yang lainnya tersimpan dampak negatifnya seperti kejahatan online atau *hacking* (peretasan), carding pada sebuah aplikasi. Maka dari itu setiap aplikasi harus dilakukan analisis manajemen risiko secara berkala agar meminimalisir kesalahan program atau *buging* serta kelemahan pada program aplikasi, yang bertujuan untuk mengetahui kelemahan - kelemahan atau kemugkinan - kemungkinan risiko yang akan terjadi dari sebuah aplikasi dan memberikan rekomendasi atau saran dari kemungkinan - kemungkinan risiko yang akan terjadi tersebut,

SINTESA merupakan sebuah aplikasi perpustakaan di XYZ yang berfungsi sebagai data informasi - informasi di perpustakan tersebut seperti mencatat buku pinjaman, daftar buku yang tersedia, jumlah buku, jatuh tempo peminjaman buku, dan daftar peminjam buku dan data petugas yang melayani pada saat itu. Dengan hadirnya SINTESA ini dapat mempermudah perpustakan untuk rekap data – data buku dan peminjamnya serta data - data lain yang terkait.

Dengan menerapkan aplikasi SINTESA ini pasti memiliki berbagai kemungkinan-kemungkinan risiko yang akan terjadi di kemudian hari yang mengganggu aktivitas aplikasi tersebut tidak berjalan secara optimal. Berdasarkan permasalahan ini, maka dibutuhkan penelitian mengenai kemungkinan - kemungkinan risiko yang akan terjadi di kemudian hari. Sehingga untuk meminimalisir kemungkinan risiko itu dapat dilakukan analisis manajemen risiko menggunakan ISO 31000.

Analisis risiko menggunakan ISO 31000 sudah dilakukan juga pada sistem aplikasi ITOP yang diteliti oleh Aprilia Rahmawati dan menghasilkan 17 kemungkinan – kemungkinan risiko yang berpotensi menganggu kinerja sistem ITOP yang di kelompokkan berdasarkan level risikonya (Rahmawati and Wijaya 2019)

Penelitian manajemen risiko menggunakan International Organization for Standardization (ISO) 31000 yang bertujuan untuk menganalisis aplikasi VCare di PT Visionet Data Internasional 20 kemungkinan risiko yang berpotensi mengganggu kinerja aplikasi VCare yang di kelompokkan berdasarkan level risikonya (Hutabarat and Manuputty 2020)

Analisis risiko yang dilakukan oleh Grialdo Willy Lantang mengenai aplikasi SAP di PT serasa Auto raya yang berpedoman dengan framework ISO 31000 dan menghasilkan 15 kemungkinan – kemungkinan risiko yang berpotensi menganggu aplikasi SAP (Lantang, Cahyono, and Ngalumsine 2019)

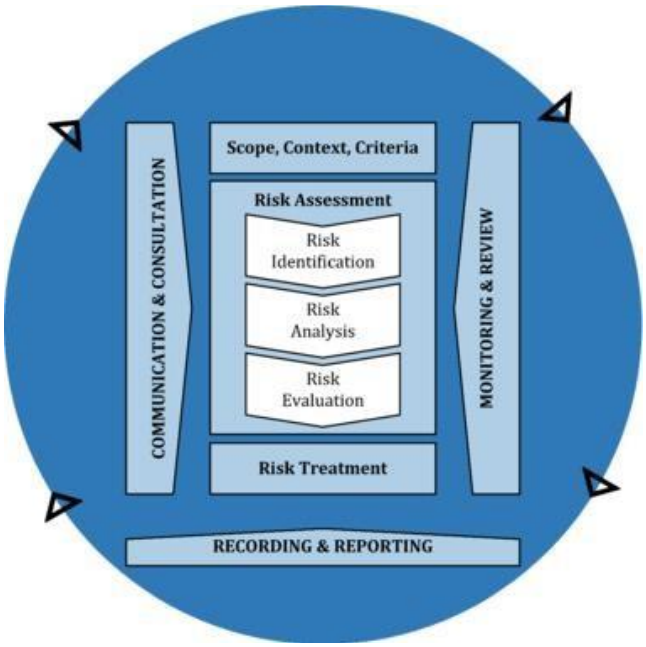
Penelitian mengenai analisis risiko website SWIFTS pada Lembaga penerbangan dan Antariksa Nasional (LAPAN) yang diteliti oleh nice dan imbar pada tahun 2017 dengan berpedoman dengan Framework ISO 31000 dan menghasilkan 43 kemungkinan - kemungkinan risiko yang dikategorikan berdasarkan sumber daya asset. (Nice and Imbar 2017)

Analisis manajemen risiko pada smart Canteen menggunakan ISO 31000 yang diteliti oleh Dewangga, yang menghasilkan beberapa kemungkinan – kemungkinan risiko yang di kelompokkan berdasarkan *level risk* (level risiko). (Ramadhan, Febriansyah, and Dewi 2020)

Berdasarkan penelitian-penelitian terdahulu, dapat di simpulkan bahwa analisis manajemen risiko menggunakan ISO 31000 bertujuan mengidentifikasi kemungkinan - kemungkinan risiko yang akan terjadi seperti, dampak risiko, level risiko dan perlakuan terhadap risiko pada sebuah perusahaan atau instansi yang diteliti. Dengan begitu penelitian analisis manajemen risiko pada sebuah perusahaan atau instansi yang diteliti merupakan hal yang sangat penting untuk menjaga aset dan aplikasi yang digunakan supaya tidak mengalami gangguan dan menganggu jalannya proses bisnis di suatu instansi atau perusahaan. Tujuan dan manfaat dari penelitian ini adalah membantu perpustakaan dalam menganalisis kemungkinan – kemungkinan risiko pada aplikasi SINTESA yang akan terjadi di kemudian hari, sehingga perpustakan dapat melakukan pencegahan sedini mungkin agar kemungkinan-kemungkinan risiko tersebut tidak terjadi dan menganggu proses bisnis di perpustakaan.

2. METODOLOGI PENELITIAN

Dalam penelitian ini menggunakan *Framework* ISO atau *International Organization for Standardization* (ISO) 31000, yang merupakan standar internasional yang mengenai atau berkaitan tentang manajemen risiko. Tujuan dari *framewor*k ISO ini adalah untuk memberikan pedoman dan prinsip - prinsip manajemen risiko yang di akui dengan lingkup yang luas. Pada gambar 1, menjelaskan susunan standar kerangka kerja dari manajemen risiko. Berdasarkan *International Organization For Standardization* (ISO 31000 :2018), maka penelitian ini akan di lakukan dalam dua tahap yaitu, tahap pertama peneliti melakukan pencarian informasi yang dibutuhkan dan diperoleh melalui pendekatan wawancara terhadap narasumber internal Perpustakaan XYZ, dan tahap ke dua, peneliti melakukan pengolahan data wawancara yang kemudian di analisa berdasarkan proses atau tahapan pada kerangka kerja ISO 31000. Didalam kerangka kerja ISO 31000 terdapat dua tahapan yaitu: di dalam tahapan pertama *Risk assessment* (penilaian), terdapat tiga proses yaitu: *Risk Identification* (identifikasi risiko) pada tahap ini bertujuan untuk mengidentifikasi komponen atau aset yang berkaitan dengan objek kasus, *Risk analyst* (analisis risiko) pada tahap ini bertujuan untuk mengelompokkan kemungkinan risiko dan dampaknya berdasarkan tabel *Likelihood* dan *Impact* , dan *Risk evaluation* (evaluasi risiko) tahap ini bertujuan untuk mengelompokkan kemungkinan-kemungkinan risiko berdasarkan level risikonya. Pada tahapan kedua ada tahap *Risk treatment* (perlakuan risiko) yang mana didalam tahapan ini peneliti memberi rekomendasi atau tindakan risiko yang bertujuan menangani kemungkinan– kemungkinan risiko tersebut.



Gambar 1. Kerangka Kerja ISO 31000 Risk manajemen.

Metode yang gunakan dalam penelitian ini adalah *Case study research,* yang dimana metode ini berfokus pada satu objek studi kasus. Dengan menerapkan metode *case study research* ini, peneliti dapat lebih fokus kepada objek penelitian secara lebih mendalam dan dapat mengumpulkan data yang dibutuhkan dengan lebih terarah serta menjawab mengenai permasalahan yang terjadi. Data yang digunakan dalam penelitian ini adalah data primer yang bersumber dari narasumber langsung atau orang yang terkait tentang SINTESA (sistem informasi Perpustakaan XYZ).

Narasumber dalam penelitian ini ada 2 yaitu: yang pertama seorang Kepala Bagian Perpustakaan (salah satu pengguna aplikasi SINTESA) dan yang kedua staf TI-PD atau orang yang bertanggung jawab terhadap *maintenance system* SINTESA. Kedua narasumber tersebut sebagai sumber data dari penelitian yang dilakukan di Perpustakaan XYZ

3. HASIL DAN PEMBAHASAN

1. Tahap Penilaian risiko (*Risk Assement*)

Pada tahap ini Proses penilaian risiko aplikasi SINTESA ini terdiri dari 3 tahap yang sesuai dengan analisis manajemen risiko ISO 31000, yaitu: Identifikasi risiko (*risk identification*), analisis risiko (*risk analysis*), evaluasi risiko (risk evaluation).

1.1. Identifikasi risiko *(risk identification)*

Tahap pertama ini, yang harus dilakukan adalah identifikasi asset yang berhubungan dengan aplikasi SINTESA. Dan dalam identifikasi ini melibatkan atau mewawancarai seorang Kepala Bagian Perpustakaan (salah satu pengguna aplikasi SINTESA) dan staf TI-PD atau bagian yang mengurusi *maintenance* sistem SINTESA. pada tahap ini memfokuskan pada asset data, software dan *Hardware*nya.

Tabel 1. Identifikasi Aset SINTESA

Komponen Sistem Informasi	ASet SINTESA
Software	Aplikasi Sintesa
Data	Data buku, data *User*
Hardware	Server database, Personal Computer

Sumber: Diolah oleh Peneliti

Setelah melakukan identifikasi risiko yang menghasilkan informasi dari data, *softwar*e, dan *Hardware* yang beruhubungan dengan aplikasi SINTESA, maka selanjutnya perlu dilakukan identifikasi kemungkinan - kemungkinan risiko yang mengancam aplikasi SINTESA. Terdapat beberapa risiko yang di kelompokan berdasarkan 3 faktor yaitu; faktor alam/lingkungan, manusia dan faktor sistem dan infrastruktur. Yang bisa dilihat pada tabel 2. dibawah ini.

Faktor	ID	Kemungkinan risiko
Alam/lingkungan	R001	Banjir
	R002	Gempa Bumi
	R003	Petir
	R004	Kebakaran
Manusia	R005	*Human Error*
	R006	Penyalahgunaan Hak Akses
	R007	*UI design* Yang Sulit Dipahami
	R008	Pencurian Data/Perangkat Keras
	R009	*Cybercrime*
	R010	*Hacking*
	R011	*Trouble Webservice*
Sistem Dan Infrastruktur	R012	Koneksi Jaringan Bermasalah
	R013	Kerusahaan *Hardware*
	R014	*Overheat*
	R015	Listrik Mati Secara Tiba- Tiba
	R016	*Data Corrupt*
	R017	*Server Down*
	R018	*Trouble Backup*

Tabel 2. Identifikasi Kemungkinan Risiko

Dari tahapan identifikasi risiko, ditemukan ada 18 kemungkinan – kemungkinan risiko yang berasal dari ketiga faktor tadi yaitu: alam/lingkungan, manusia, sistem dan infrastruktur yang

mengancam aplikasi SINTESA. Setelah di ketahui kemungkinan risikonya pada tahapan ini juga mengalukukan indentifikasi dampak - dampak dari kemungkinan-kemungkinan risiko tadi. Yang dapat dilihat pada tabel 3.

Tabel 3. Identifikasi dampak risiko.

ID	Kemungkinan risiko	dampak
R001	Banjir	Aktivitas kegiatan perpustakaan tergangu
R002	Gempa Bumi	Kerusakan infrastruktur dan aktivitas kegiatan perpustakaan tergangu
R003	petir	Kerusakan Infrastruktur perpustakaan
R004	Kebakaran	Kerusakan Infrastruktur aktivitas kegiatan perpustakaan Berhenti
R005	*Human Error*	Proses layanan Perpustakaan tidak berjalan dengan optimal
R006	Penyalahgunaan hak akses	Data diri *User* akan tersadap atau hak *User* akan disalah gunakan
R007	*UI design* sulit dipahami	*User* kesulitan dalam memahami atau menjalan aplikasi
R008	Pencurian data/perangkat keras	Perpustakaan akan mengalami kerugian karena kehilangan data dan perangkat keras
R009	*Cybercrime*	Bocornya informasi atau data perpustakaan
R010	*hacking*	Sistem akan disadap dan mengalami gangguan
R011	Trouble Web server	Aplikasi SINTESA tidak dapat di akses
R012	Koneksi jaringan bermasalah	Terhambat atau kesulitan dalam mengakses aplikasi SINTESA
R013	Kerusakan *Hardware*	Menghambat kinerja/ aktivitas di perpustakaan karena harus melakukan konfigurasi di *Hardware* baru
R014	*Overheat*	*Hardware* mengalami gangguan atau *Trotling* (penurunan performa karena suhu meningkat)

R015	Listrik mati secara tiba - tiba	Tidak berpengaruh karena perpustakaan ada cadangan listrik (Genset)
R016	*Data Corrupt*	Perpustakaan tidak dapat melihat atau mendapatkan data yang valid
R017	*Server Down*	Tidak dapat mengakses aplikasi dan data base SINTESA dan menghambat aktivitas perpustakaan
R018	*Trouble Backup*	Data tidak dapat dibackup yang menyebabkan kerugian bagi Perpustakaan

1.2. Analisis risiko *(Risk analysis)*

setelah selelai melakukan proses identifikasi risiko dan dampaknya, selanjutnya melakukan analisis risiko. Pada tahapan ini dilakukan penilaian terhadap kemungkinan-kemungkinan risiko yang sudah di identifikasi pada tahapan sebelumnya dengan menggunakan tabel kriteria *Likelihood* dan tabel *Impact*, sebagai acuan untuk melakukan analisis risiko. Pada tabel *Likelihood* terdapat 4 kriteria yang berdasarkan seringnya kemungkinan risiko terjadi.

Tabel 4. *Likelihood*

Likelihoad			
Nilai	Kriteria	Deskrispi	Frekuensi kejadian
1	Rare	Resiko tersebut hampir tidak pernah terjadi	> 2 Tahun
2	Unlikely	resiko tersebut jarang terjadi	1 - 2 tahun
3	Possible	resiko tersebu kadang terjadi	7 - 12 bulan
4	Likely	resiko tersebut sering terjadi	4 - 6 bulan
5	Certain	Resiko tersebut pasti terjadi	1 - 3 bulan

Dan di tabel 5 dibawah ini merupakan tabel penilaian *impact* dampak yang terjadiakibat dari risiko - risiko tadi jika terjadi di perpustakaan. Pada tabel 5 ini kriteria dampak di kelompokkan berdasarkan 5 kriteria. Dan di kelempokkan berdasarkan dampak yang tidak berpengaruh dan dampak yang paling berpengaruh terhadap Perpustakaan. Bisa dilihat di tabel 5 dibawah ini.

Tabel 5. *Impact*

Impact		Keterangan
Nilai	Kriteria	
1	Insignificant	tidak mengaggu aktivitas perpustakaan
2	Minor	aktivitas perusahaan sedikit terhambat namun aktivitas inti perpustakaan tidak mengaggu
3	Moderate	menyebabkan gangguan pada proses bisnis sehingga sebagian jalannya aktivitas perpustakaan terhambat
4	Major	menghambat hampir seluruh aktivitas Perpustakaan
5	Catasirophic	aktivitas perusahaan berhenti karena proses bisnis mengalami gangguan total

Setelah mendapatkan nilai kemungkinan (*Likelihood*) di tabel 4. Dan dampak (*Impact*) di tabel 5. Maka selanjutnya dilakukan penilaian terhadap kemungkinan – kemungkinan risiko yang ada di sekitar aset aplikasi SINTESA yang sudah teridentifikasi pada tahapan sebelumnya. Untuk melihat penilaian kemungkinan -kemungkinan risiko itu dapat dilihat pada tabel 6 berikut.

Tabel 6, Penilaian Kemungkinan risiko

Faktor	ID	Kemungkinan resiko	Likelihood	Impact
alam/lingkungan	R001	banjir	1	2
	R002	gempa bumi	2	5
	R003	petir	3	2
	R004	kebakaran	1	5
Manusia	R005	Human error	4	3
	R006	Penyalahgunaan hak akses	2	1
	R007	UI design yang sulit dipahami	1	1
	R008	Pencurian data/perangkat keras	2	2
	R009	cybercrime	2	2
	R010	Hacking	2	2
	R011	Trouble webservice	4	5
system dan infrastruktur	R012	koneksi jaringan bermasalah	5	4
	R013	kerusahaan hardware	2	4
	R014	overheat	3	3
	R015	listrik mati secara tiba- tiba	4	3
	R016	data corrupt	1	2
	R017	server down	3	4
	R018	Trouble backup	1	2

1.3. Evaluasi risiko *(Risk evaluation)*

Pada tahapan ini akan dilakukan proses evaluasi risiko dari kemungkinan - kemungkinan risiko yang sudah di analisis pada tahapan sebelumnya. Dari hasil analisis tersebut akan dimasukkan ke dalam matriks evaluasi risiko berdasarkan pedoman yang ada di dalam kerangka kerja ISO 31000. Matriks evaluasi dibedakan menyadi 3 level risiko yaitu: *Low, Medium,* dan *high*. Kemungkinan - kemungkinan risiko sebelumnya yang sudah di nilai dengan menilai kemungkinannya dan dampaknya pada tahapan sebelumnya yang di sesuaikan pada matriks evaluasi. Hasil dari penilaian risiko berdasarkan *Likelihood* dan *Impact* dapat dilihat pada tabel 7 dibawah ini.

Tabel 7. 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

Pada tabel 8 di bawah ini dilakukan evaluasi risiko berdasarkan dari identitas atau ID kemungkinan – kemungkinan risiko, untuk dimasukkan kedalam matriks evaluasi sesuai dengan kriteria *Likelihood* dan kriteria *Impact.*

Tabel 8 matriks evaluasi risiko berdasarkan *Likelihood* dan *impact*

Likelihood						
Certain	5				R012	
Likely	4			R005 R015		R011
Possible	3		R003	R014	R017	
Unlikely	2	R006	R008 R009 R010		R013	R002
Rare	1	R007	R001 R016 R018			R004
Impact		1	2	3	4	5
		Insignificant	Minor	Moderate	Major	Catastrophic

Setelah memasukan kemungkinan – kemungkinan risiko tadi kedalam matriks evaluasi berdasarkan *Likelihood* dan *impact* maka pada tahapan berikutnya pada tabel 9 akan di dikelompokkan 18 kemungkinan risiko diatas kedalam tingkatan level *high*, *medium* dan *low*.

Tabel 9. Pengelompokan risiko berdasarkan tingkatan level

ID	kemungkinan resiko	Likelihood	Impact	Risk Level
R011	Trouble Web service	4	5	HIGH
R012	Koneksi jaringan bermasalah	5	4	HIGH
R002	Gempa Bumi	2	5	MEDIUM
R004	Kebakaran	1	5	MEDIUM
R005	Human error	4	3	MEDIUM
R013	Kerusakan hardware	2	4	MEDIUM
R014	Overheat	3	3	MEDIUM
R015	listrik mati tiba-tiba	4	3	MEDIUM
R017	server down	3	4	MEDIUM
R001	Banjir	1	2	LOW
R006	penyalahgunaan hak akses	2	1	LOW
R007	UI design yang sulit dipahami	1	1	LOW
R008	Pencurian data/Perangkat keras	2	2	LOW
R009	Cybercrime	2	2	LOW
R010	Hacking	2	2	LOW
R016	Data Corrupt	1	2	LOW
R018	Trouble Backup	1	2	LOW

Dari tahapan proses evaluasi risiko ini, terdapat 18 kemungkinan risiko yang sudah di identifikasi dan analisis serta di kelompokkan berdasarkan level risikonya. Terdapat 2 kemungkinan risiko yang masuk kedalam risk level tingkatan *high*, yaitu: R011 (Trouble Web Service) dan R012 (Koneksi Jaringan Bermasalah), terdapat 7 kemungkinan risiko yang masuk kedalam level tingkatan *medium*, yaitu: R002 (Gempa bumi), R004 (Kebakaran), R005 (*Human Error*), R013 (kerusakan *Hardware*), R014 (*Overheat*), R015 (Listrik mati Tiba-tiba), dan R017 (*Server down*). Serta terdapat 8 kemungkinan risiko yang masuk kedalam risk level tingkatan *Low*, yaitu; R001 (banjir), R006 (Penyalahgunaan hak akses), R007 (*UI design* yang sulit dipahami), R008 (Pencurian data/Perangkat keras), R009 (*Cybercrime*), R010 (*Hacking*), R016 (*Data Corrupt*), dan R018 (*Trouble Backup*).

2. Perlakuan Risiko (*Risk treatment*)

setelah melakukan proses atau tahapan (identifikasi risiko) mengenai aset - aset yang berada dalam lingkungan aplikasi SINTESA, maka selanjutnya akan dilakukan proses *Risk treatment* atau perlakuan risiko yang dimana dalam tahap ini memberikan Tindakan risiko terhadap kemungkinan – kemungkinan risiko yang sudah di kelompokkan berdasarkan level risiko. Dan usulan perlakuan risiko dan diihat di tabel 10. Dibawah ini.

Tabel 10. Usulan Perlakukan risiko

ID	kemungkinan risiko	Risk Level	Tindakan Risiko
R011	Trouble Web service	*HIGH*	Membuat SOP untuk menangani Trouble web Service dan memberikan notification ke *User* mengenai trouble web service
R012	Koneksi jaringan bermasalah	*HIGH*	Mengganti ISP *(Internet service Provider)* baru
R002	Gempa Bumi	*MEDIUM*	Menyediakan akau menyiapkan Server cadangan
R004	Kebakaran	*MEDIUM*	Menyiapkan alat – alat yang mencegah kebakaran
R005	*Human Error*	*MEDIUM*	Melakukan training kepada *User- User*
R013	Kerusakan *Hardware*	*MEDIUM*	Memberikan asuransi terhadap semua *Hardware* yang ada
R014	*Overheat*	*MEDIUM*	Menyediakan ruang yang memiliki (Air Conditioner) dan menambah pendingin pada semua *Hardware*
R015	listrik mati tiba-tiba	*MEDIUM*	Menyediakan UPS atau generator sesuai kebutuhan
R017	*Server Down*	*MEDIUM*	Melakukan pengecek berkala pada database perpustakaan
R001	Banjir	*LOW*	Meletakkan alat – alat vital di tempat yang aman dari banjir

R006	penyalahgunaan hak akses	*LOW*	Memberikan batasan 1 *User* 1 device atau memberikan konfirmasi login yang berkaitan dengan pribadi *User*
R007	*UI design* yang sulit dipahami	*LOW*	Mengubah tampilan *User* interface agar lebih simple dan fungsional dan penggunaan warna icon yang simple
R008	Pencurian data/Perangkat keras	*LOW*	Meletakan alat security seperti cctv, alarm, dan alat sensor di setiap ruangan.
R009	*Cybercrime*	*LOW*	Menggunakan jaringan private agar sulit untuk diretas
R010	*Hacking*	*LOW*	Melakukan pergantian password akun secara berkala. Dan meningkatkan sistem securitynya
R016	*Data Corrupt*	*LOW*	Menggunakan aplikasi -aplikasi original dan melakukan backup data secara berkala setelah melakukan penginputan.
R018	*Trouble Backup*	*LOW*	Membuat SOP tentang jadwal backup yang berkala Dan membuat SOP mengenai trouble backup.

4. KESIMPULAN

Berdasarkan penelitian analisis risiko teknologi informasi menggunakan ISO 31000 yang sudah dilakukan pada sebuah aplikasi perpustakaan yang bernama SINTESA, dan sudah melalui semua tahapan, dari penilaian risiko, identifikasi risiko, analisis risiko, tahap evaluasi risiko, hingga tahap perlakukan risiko. Dari tahapan-tahapan tersebut analisis risiko manajemen ini mendapatkan 18 kemungkinan – kemungkinan risiko yang akan menganggu kinerja dari aplikasi SINTESA di perpustakan XYZ. Terdapat 2 kemungkinan risiko dengan kategori *risk level High* yaitu: R011 (Trouble web service) dan R012 (Koneksi jaringan bermasalah). Selanjutnya terdapat 7 kemungkinan risiko dengan kategori *risk level medium* yaitu: R002 (Gempa bumi), R004 (Kebakaran), R005 (*Human Error*), R013 (Kerusakan *Hardware*), R014 (*Overheat*), R015 (Listrik Mati tiba-tiba), R017 (*Server Down*). Serta terdapat 8 kemungkinan risiko dengan kategori *risk level Low* yaitu: R001 (Banjir), R006 (Penyalahgunaan Hak akses), R007 (*UI design* sulit dipahami), R008 (Pencurian data/perangkat keras), R009 (*Cybercrime*), R010 (*Hacking*), R016 (*Data corrupt*), R018 (*Trouble Backup*). kemungkinan – kemungkinan risiko diatas yang dikategorikan yang terjadi disebabkan oleh faktor alam dan manusia yang kedepannya jika tidak diperbaiki dan diperlakukan dengan baik akan menimbulkan masalah unutk aplikasi sintesa di perpustakan XYZ

Dengan demikian diharapkan penelitian ini dapat digunakan perpustakaan XYZ dalam Menyusun Standar Operasional Prosedur atau kebijakan untuk meminimalisir kemungkinan - kemungkinan risiko diatas terjadi dan menganggu sistem aplikasi SINTESA.

Referensi

Hutabarat, Felisia Meini, and Augie David Manuputty. 2020. "Analisis Risiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000." *Jurnal Bina Komputer* 2(1):52–65.

Lantang, Grialdo Willy, Ariya Dwika Cahyono, and Nikolar Ngalumsine. 2019. "Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di Pt Serasi Autoraya Menggunakan ISO 31000." *Sebatik 2621-069X* 23 No. 1:36–43.

Nice, Francisca Lady, and Radiant Victor Imbar. 2017. "Analisis Risiko Teknologi Informasi Pada Lembaga Penerbangan Dan Antariksa Nasional (LAPAN) Pada Website SWIFTS Menggunakan ISO 31000." *Jurnal Informatika Dan Sistem Informasi* 2(2):1–11.

Rahmawati, Aprilia, and Agustinus Fritz Wijaya. 2019. "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP." *Jurnal SITECH: Sistem Informasi Dan Teknologi* 2(1):13–20.

Ramadhan, Dewangga Lazuardi, Ronie Febriansyah, and Renny Sari Dewi. 2020. "Analisis Manajemen Risiko Menggunakan ISO 31000 Pada Smart Canteen SMA XYZ." *JURIKOM (Jurnal Riset Komputer)* 7(1):91.