ANALISIS MANAJEMEN RISIKO SITUS WEB OPAC PADA PERPUSTAKAAN UIN SUNAN AMPEL SURABAYA

Mohammad Adam Malik, Khalid, Faris Mushlihul Amin
Sistem Informasi, Universitas Islam Negeri Sunan Ampel Surabaya
Jl. Dr. Ir. H. Soekarno No.682 Surabaya, Indonesia
madammalik01@gmail.com

ABSTRAK

Dalam era pesatnya kemajuan teknologi informasi, peran perpustakaan dalam menyediakan akses efisien dan mudah ke koleksi perpustakaan dan sumber daya informasi menjadi semakin penting. Namun, dengan peralihan ke dunia digital, perpustakaan dihadapkan pada tantangan signifikan, termasuk risiko terkait dengan keamanan data, gangguan teknis, dan masalah manajemen konten. Untuk mengatasi risiko – risiko ini, penelitian ini menerapkan *framework* ISO 31000 dan memanfaatkan konsep *likelihood* (kemungkinan) dan impact (dampak). Penelitian ini mencakup langkah–langkah analisis risiko yang komprehensif, yang bertujuan untuk mengidentifikasi dan mengevaluasi berbagai risiko yang mungkin muncul selama operasional situs web *Public Access Catalog*. Selain itu, penelitian ini juga mengeksplorasi strategi manajemen risiko yang telah diterapkan atau diusulkan untuk menangani tantangan–tantangan yang dihadapi oleh perpustakaan. Penelitian ini berhasil mengidentifikasi 14 potensi risiko dengan kategori tinggi *(high)*, sedang *(medium)*, dan rendah *(low)*. Penelitian ini dapat memberikan rekomendasi praktis untuk meningkatkan manajemen risiko di lingkungan digital perpustakaan. Dengan pengetahuan yang diperoleh dari penelitian ini, juga dapat menjadi acuan perpustakaan lain akan mendapatkan wawasan berharga dalam menghadapi tantangan serupa dalam lingkungan digital yang terus berkembang. Dengan demikian, penelitian ini menjadi kontribusi penting dalam upaya meningkatkan kualitas dan keamanan layanan perpustakaan di era digital yang penuh kompleksitas dan risiko.

Kata kunci : *ISO 31000, Manajemen Risiko, Teknologi Informasi, Website, Analisis Risiko, Penilaian Risiko*

1. PENDAHULUAN

Dengan pesatnya perkembangan teknologi informasi, peran perpustakaan dalam memastikan akses public yang efisien dan mudah ke koleksi perpustakaan serta sumber daya informasi semakin krusial. Terutama di era di mana informasi menjadi lebih mudah diakses dan dibagikan secara digital, perpustakaan sebagai institusi pendidikan dan pengetahuan perlu menyesuaikan diri dengan perubahan ini. Hal ini berlaku pula untuk Perpustakaan UIN Sunan Ampel Surabaya, sebuah institusi akademik yang berkomitmen kuat untuk memberikan layanan terbaik kepada mahasiswanya dan masyarakat umum. Teknologi informasi adalah komponen dari upaya yang menggunakan perangkat elektronik komputer. Secara umum, teknologi informasi mengacu pada teknologi yang utamanya memanfaatkan komputer sebagai alat utama untuk mengubah data menjadi informasi bernilai [1].

Untuk memenuhi tuntutan pelayanan informasi yang lebih canggih, perpustakaan memanfaatkan teknologi digital, di mana situs web *Public Access Catalog* (OPAC) berperan penting sebagai alat yang memfasilitasi akses ke koleksi perpustakaan dan membantu pengguna menjelajahi informasi. Meskipun OPAC menawarkan banyak manfaat, terdapat risiko yang perlu diperhatikan, seperti keamanan data, gangguan teknis, dan masalah manajemen konten. Oleh karena itu, pengelolaan risiko yang efektif sangat penting untuk memastikan fungsi optimal situs web dan perlindungan aset berharga. Jurnal ini bertujuan untuk mendokumentasikan dan menganalisis pendekatan manajemen risiko yang diterapkan dalam pengelolaan OPAC di Perpustakaan UIN Sunan Ampel Surabaya, serta mengidentifikasi risiko dan mengeksplorasi strategi manajemen yang diusulkan untuk mengatasi tantangan tersebut.

Untuk mencapai penelitian ini, kami akan merinci langkah–langkah analisis risiko yang telah kami terapkan dalam lingkungan perpustakaan digital ini. Penulis akan membagikan hasil temuan kami seputar risiko–risiko yang kami identifikasi dan evaluasi, serta memberikan rekomendasi praktis untuk meningkatkan manajemen risiko di lingkungan digital perpustakaan. Tujuan utama dari penelitian ini adalah memberikan wawasan yang berharga bagi para praktisi dan peneliti di bidang perpustakaan digital serta manajemen risiko teknologi informasi.

2. TINJAUAN PUSTAKA

Pada tahun 2020, Sukma Arta Atmojo dan Augie David Manuputty melakukan sebuah penelitian yang berfokus pada penggunaan ISO 31000 dalam mengelola risiko teknologi informasi pada aplikasi AHO. Penelitian ini bermaksud untuk secara terperinci mendokumentasikan risiko–risiko yang mungkin muncul dalam penggunaan aplikasi AHO, serta menganalisis tingkat dampak dari risiko-risiko tersebut. Selain itu, penelitian ini juga berupaya memberikan rekomendasi mengenai Langkah-langkah perlakuan risiko yang dapat diambil untuk mengelola risiko-risiko tersebut secara efektif. Dengan demikian, penelitian tersebut memberikan pandangan mendalam tentang cara menghadapi risiko dalam konteks

Teknologi Informasi dan aplikasi AHO. Hasil penelitian terhadap aplikasi AHO menunjukkan adanya 19 potensi risiko yang dapat mempengaruhi performa aplikasi tersebut, di mana 3 di antaranya masuk dalam kategori resiko ekstrim, 7 di antaranya termasuk dalam kategori risiko tinggi, 7 di antaranya termasuk dalam kategori risiko sedang, dan 2 di antaranya termasuk dalam kategori risiko rendah [2].

2.1. Risiko

Risiko merupakan probabilitas atau kemungkinan terjadinya peristiwa yang berpotensi memberikan dampak negatif pada perusahaan. Risiko, pada dasarnya, merujuk kepada kejadian atau situasi yang, jika terjadi, dapat memiliki konsekuensi merugikan terhadap tujuan dan strategi perusahaan. Maka, hal ini menjadi penting untuk secara cermat mengidentifikasi dan mengukur baik kemungkinan terjadinya risiko maupun dampak yang mungkin timbul pada bisnis, karena hal ini merupakan aspek mendasar dalam pengelolaan risiko Perusahaan. Jadi definisi dari risiko adalah hasil dari gabungan antara probabilitas terjadinya suatu peristiwa dan dampaknya. Tingkat risiko secara umum ditentukan oleh berbagai faktor, yang meliputi sejauh mana paparan, lokasi, jumlah pengguna, jumlah, serta kerentanan elemen yang terlibat dalam situasi tersebut [3].

2.2. Manajemen Risiko

Manajemen risiko merupakan suatu proses yang mencakup pengidentifikasian, analisis, evaluasi, pengendalian, serta usaha untuk mencegah, mengurangi, atau bahkan menghilangkan risiko yang tidak dapat diterima [4].

Manajemen risiko dilakukan untuk melindungi perusahaan dari risiko yang menghalau pencapaian tujuan dan berbagai hal yang berpotensi merugikan Perusahaan. Manajemen risiko diharapkan dapat berfungsi sebagai alat bantu bagi Perusahaan dalam pengambilan keputusan yang akurat untuk mengurangi potensi kerugian [5].

2.3. Proses Manajemen Risiko

Menurut ISO 31000:2009, disebutkan bahwa proses manajemen risiko dianggap sebagai komponen kunci dalam manajemen risiko, karena melibatkan penerapan prinsip dan kerangka kerja yang telah ada sebelumnya. Manajemen risiko terbagi menjadi tiga tahap inti, yaitu:

a. Menentukan konteks (establishing the context)
b. Penilaian risiko (risk assessment)
c. Pengelolaan risiko (risk treatment)

Dalam menjalankan proses manajemen risikonya, ISO 31000 mengklasifikasikan kriteria risiko berdasarkan tingkat signifikansinya [6]. ISO 31000:2018 menggantikan edisi tahun 2009, dengan mengubah istilah dari “prinsip dan pedoman” menjadi “pedoman”. Ini merupakan Langkah penyederhanaan dari versi sebelumnya, yang tercermin dari penurunan jumlah halaman dari 24 halaman menjadi hanya 16 halaman [7].

2.4. *Framework* ISO 31000

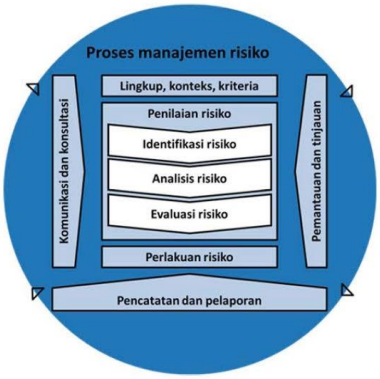
ISO 31000, sebuah standar manajemen risiko, merupakan salah satu dari rangkaian standar internasional yang memberikan panduan untuk manajemen risiko dan dikeluarkan oleh Organisasi Internasional untuk Standardisasi. Standar ini dikeluarkan pada tanggal 13 November 2009 sebagai perkembangan dari standar sebelumnya, yaitu AS/NZS 4360:2004 yang diterbitkan oleh Standar Australia. Seperti kebanyakan standar manajemen ISO lainnya, ISO 31000 menyediakan kerangka kerja terstruktur yang dimaksudkan untuk memenuhi kebutuhan semua jenis organisasi atau situasi [8].

Salah satu perbedaan signifikan antara ISO 31000 dan standar manajemen risiko lainnya terletak pada cakupan yang lebih luas dan konsep yang lebih inklusif. Hal ini dapat dilihat dalam penerapan kerangka kerja manajemen risiko yang mengadopsi prinsip-prinsip manajemen mutu yang dikenal dengan nama "Plan-Do-Check-Act” [9].

3. METODE PENELITIAN

Dalam studi ini, peneliti menggunakan ISO 31000 *framework*, yang merupakan kerangka kerja dari *International Organization for Standardization* (ISO), yang merupakan standar global yang berkaitan dengan manajemen risiko [10].

ISO 31000 dibuat dengan tujuan memberikan pedoman dan prinsip-prinsip manajemen risiko yang diakui secara umum dengan cakupan yang mendalam. Berdasarkan ISO 31000:2018 dari Organisasi Internasional untuk Standardisasi, penelitian ini akan dilakukan dalam dua tahap. Tahap awal akan melibatkan pengumpulan informasi yang diperlukan melalui wawancara dengan narasumber internal di Perpustakaan UIN Sunan Ampel Surabaya. Sementara itu, langkah kedua akan melibatkan pemrosesan data wawancara yang akan dianalisis sesuai dengan prosedur-prosedur yang tercantum dalam kerangka kerja ISO 31000.



Gambar 1. Kerangka Kerja ISO 31000

Kerangka kerja ISO 31000 terdiri dari dua tahapan utama. Tahap awal adalah penilaian risiko,

yang melibatkan tiga proses inti. Sebagai langkah pertama yaitu identifikasi risiko *(risk identification)*, langkah kedua adalah analisis risiko *(risk analysis)*, dan langkah ketiga yaitu evaluasi risiko *(risk evaluation)*. Tahap kedua dalam kerangka kerja ISO 31000 adalah penanganan risiko *(risk treatment)*, di mana peneliti memberikan rekomendasi atau tindakan untuk mengatasi risiko yang telah teridentifikasi.

Dalam penelitian ini, digunakan metode *case study research*. Pendekatan ini berfokus pada satu subjek studi kasus, yang dalam konteks ini adalah katalog akses publik daring Perpustakaan UIN Sunan Ampel Surabaya. Melalui penerapan metode *case study research*, peneliti memiliki kesempatan untuk menggali lebih dalam pemahaman terhadap objek penelitian dan mengumpulkan data yang lebih relevan dengan fokus yang lebih terarah. Selain itu, metode ini memungkinkan peneliti untuk menjawab permasalahan yang muncul dengan lebih baik. Data yang digunakan dalam penelitian ini adalah data primer yang diperoleh secara langsung dari pihak-pihak yang terkait dengan Sistem Informasi Katalog Perpustakaan UIN Sunan Ampel Surabaya, yang dikenal sebagai *Web Online Public Access Catalog.* Dua narasumber utama dalam penelitian ini adalah, sebagai berikut :

a. Kepala bagian Perpustakaan, yang juga salah satu pengguna *Web Online Public Access Catalog* Perpustakaan UIN Sunan Ampel Surabaya.
b. Staf TI Perpustakaan, yang bertanggung jawab terhadap pemeliharaan sistem dari *Web Online Public Access Catalog* Perpustakaan UIN Sunan Ampel Surabaya.

Kedua narasumber ini akan menjadi sumber data utama yang akan memberikan wawasan dan informasi penting yang berkaitan dengan manajemen risiko *Web Online Public Access Catalog* Perpustakaan UIN Sunan Ampel Surabaya.

4. HASIL DAN PEMBAHASAN

4.1. Identifikasi Risiko *(Risk Identification)*

Pada tahap awal ini, langkah pertama yang harus diambil adalah mengidentifikasi aset yang terkait dengan situs *Web Online Public Access Catalog.* Dalam proses identifikasi ini, melibatkan wawancara dengan Kepala bagian Perpustakaan (seorang pengguna situs *Web Online Public Access Catalog* Perpustakaan UIN Sunan Ampel Surabaya) dan staf TI atau tim yang bertanggung jawab atas pemeliharaan sistem OPAC. Pada tahap ini, perhatian difokuskan pada aset data, perangkat lunak dan perangkat keras yang terlibat.

Tabel 1. Identifikasi Aset Situs Web OPAC

Komponen Sistem Informasi	Aset Situs *Web Online Public Access Catalog* Perpustakaan UIN Sunan Ampel Surabaya
Software	Situs *Web OPAC*
Data	Data Buku, Data Pengguna
Hardware	Server *database*, Personal Laptop/*Handphone*

Setelah menyelesaikan proses identifikasi risiko yang menghasilkan informasi terkait dengan perangkat keras dan perangkat lunak yang terhubung dengan *Web Online Public Access Catalog* (OPAC) Perpustakaan UIN Sunan Ampel Surabaya, langkah berikutnya adalah mengenali potensi risiko yang dapat mengancam OPAC tersebut. Risiko-risiko ini di berbagai berdasarkan dua faktor, yaitu manusia dan sistem serta infrastruktur, seperti yang terlihat pada tabel 2 di bawah ini.

Tabel 2. Identifikasi Kemungkinan Risiko

Faktor	ID	Kemungkinan Risiko
Manusia	R001	*Human Error*
	R002	Penyalahgunaan Hak Akses
	R003	*UI Design* Yang Sulit Dipahami
	R004	Pencurian Data/Perangkat Keras
	R005	*Cybercrime*
	R006	*Hacking*
	R007	*Trouble Webserver*
Sistem dan Infrastruktur	R008	Koneksi Jaringan Bermasalah
	R009	Kerusakan *Hardware*
	R010	*Overheat*
	R011	Listrik Mati Secara Tiba-Tiba
	R012	*Data Corrupt*
	R013	*Server Down*
	R014	*Trouble Backup*

Selama proses identifikasi risiko, ditemukan total 14 potensi risiko yang muncul dari kedua faktor, yaitu manusia, sistem, dan infrastruktur, yang dapat mengancam situs web OPAC. Setelah mengetahui kemungkinan risikonya, pada tahap ini juga dilakukan identifikasi dampak yang mungkin timbul akibat risiko tersebut, seperti yang tercantum dalam tabel 3 dibawah ini.

Tabel 3. Identifikasi Dampak Risiko

ID	Kemungkinan Risiko	Dampak
R001	*Human Error*	Proses pelayanan OPAC perpustakaan tidak mencapai tingkat optimal
R002	Penyalahgunaan Hak Akses	Data identitas pengguna rentan untuk disalahkan
R003	*UI Design* Yang Sulit Dipahami	Pengguna mengalami kesulitan dalam navigasi situs web
R004	Pencurian Data/Perangkat Keras	Perpustakaan berisiko mengalami kerugian karena kehilangan data dan perangkat keras
R005	*Cybercrime*	Kebocoran informasi atau data perpustakaan
R006	*Hacking*	Sistem rentan terhadap penyadapan dan gangguan
R007	*Trouble Webserver*	Situs web OPAC tidak bisa diakses
R008	Koneksi Jaringan Bermasalah	Terjeda atau terhambat saat mencoba mengakses situs web OPAC
R009	Kerusakan *Hardware*	Mengganggu efisiensi aktivitas perpustakaan

ID	Kemungkinan Risiko	Dampak
		karena konfigurasi perangkat keras baru
R010	*Overheat*	Perangkat keras mengalami masalah atau mengalami *thermal throttling* (penurunan performa akibat suhu meningkat)
R011	Listrik Mati Secara Tiba-Tiba	Perpustakaan UIN Sunan Ampel harus memiliki sumber listrik alternatif (Genset)
R012	*Data Corrupt*	Perpustakaan kesulitan dalam mengakses atau memperoleh data yang sah
R013	*Server Down*	Masalah akses ke situs web dan database OPAC menghambat rutinitas perpustakaan
R014	*Trouble Backup*	Ketidakmampuan membuat salinan data yang menimbulkan kerugian bagi perpustakaan

4.2. Analisis Risiko *(Risk Analysis)*

Setelah menyelesaikan tahap identifikasi risiko dan penilaian dampaknya, langkah selanjutnya adalah melakukan analisis risiko. Dalam langkah ini, risiko-risiko yang sudah diidentifikasi sebelumnya dinilai dengan menggunakan tabel kriteria kemungkinan *(likelihood)* dan tabel dampak *(impact)* sebagai pedoman dalam analisis risiko. Tabel *likelihood* terdiri dari empat kriteria yang didasarkan pada frekuensi kemungkinan terjadinya risiko.

Tabel 4. Likelihood

Likelihood			
Nilai	**Kriteria**	**Deskripsi**	**Frekuensi Kejadian**
1	*Rare*	Risiko tersebut hampir tidak pernah terjadi	> 2 Tahun
2	*Unlikely*	Risiko tersebut jarang terjadi	1 - 2 Tahun
3	*Possible*	Risiko tersebut kadang terjadi	7 - 12 Bulan
4	*Likely*	Risiko tersebut sering terjadi	4 - 6 Bulan
5	*Certain*	Risiko tersebut pasti terjadi	1 - 3 Bulan

Di dalam Tabel 5 di bawah ini, terdapat evaluasi mengenai potensi dampak yang bisa terjadi sebagai akibat dari risiko-risiko yang muncul jika terjadi di perpustakaan. Dalam tabel ini, kriteria dampak dibagi ke dalam lima kategori yang memisahkan antara dampak yang rendah dan dampak yang paling signifikan terhadap Perpustakaan, seperti yang terlihat di Tabel 5 di bawah ini.

Tabel 5. *Impact*

Impact		**Keterangan**
Nilai	**Kriteria**	
1	*Insignificant*	Tidak menghambat operasi Situs Web OPAC Perpustakaan
2	*Minor*	Aktivitas situs web OPAC perpustakaan sedikit terhambat namun aktivitas inti situs web OPAC perpustakaan tidak terganggu
3	*Moderate*	Mengakibatkan penundaan dalam sebagian operasi Situs Web OPAC Perpustakaan
4	*Major*	Mengganggu hampir semua operasi Situs Web OPAC Perpustakaan
5	*Catastrophic*	Operasi Situs Web OPAC Perpustakaan berhenti sepenuhnya karena terjadi gangguan total dalam proses bisnis

Setelah mendapatkan nilai tingkat kemungkinan *(likelihood)* dari tabel 4 dan tingkat dampak *(impact)* dari tabel 5, langkah selanjutnya adalah mengevaluasi risiko-risiko yang terkait dengan aset situs web OPAC Perpustakaan UIN Sunan Ampel Surabaya yang sudah diidentifikasi pada tahap sebelumnya. Evaluasi kemungkinan risiko-risiko tersebut terdokumentasikan di tabel 6 di bawah ini.

Tabel 6. Penilaian Kemungkinan Risiko

Faktor	ID	Kemungkinan Risiko	Likelihood	Impact
Manusia	R001	*Human Error*	4	3
	R002	Penyalahgunaan Hak Akses	2	1
	R003	*UI Design* Yang Sulit Dipahami	1	1
	R004	Pencurian Data/Perangkat Keras	2	2
	R005	*Cybercrime*	2	2
	R006	*Hacking*	2	2
	R007	*Trouble Webserver*	4	5
Sistem dan Infrastruktur	R008	Koneksi Jaringan Bermasalah	5	4
	R009	Kerusakan *Hardware*	2	4
	R010	*Overheat*	3	3
	R011	Listrik Mati Secara Tiba-Tiba	4	3
	R012	*Data Corrupt*	1	2
	R013	*Server Down*	3	4
	R014	*Trouble Backup*	1	2

4.3. Evaluasi Risiko *(Risk Evaluation)*

Dalam langkah ini, evaluasi risiko dilaksanakan berdasarkan hasil analisis risiko yang telah dilakukan pada tahap sebelumnya. Hasil analisis ini akan dipresentasikan dalam bentuk matriks evaluasi risiko

sesuai dengan panduan yang terdapat dalam kerangka kerja ISO 31000. Matriks evaluasi risiko dibagi menjadi tiga tingkatan risiko : *low* (rendah), *medium* (sedang), dan *high* (tinggi). Kemungkinan risiko-risiko yang sebelumnya telah dinilai berdasarkan kemungkinan dan dampaknya pada tahap sebelumnya akan disesuaikan dengan matriks evaluasi. Evaluasi risiko berdasarkan kemungkinan *(likelihood)* dan dampak *(impact)* dapat diidentifikasi di dalam Tabel 7 di bawah 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*

Dalam Tabel 8 di bawah ini, risiko dievaluasi berdasarkan identifikasi atau ID risiko yang mematuhi panduan kriteria kemungkinan (Likelihood) dan kriteria dampak, kemudian dimasukkan ke dalam matriks evaluasi.

Tabel 8. Matriks Evaluasi Risiko berdasarkan *Likelihood* dan *Impact*

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

Setelah memasukkan risiko-risiko yang sudah teridentifikasi ke dalam matriks evaluasi berdasarkan kemungkinan *(likelihood)* dan dampak, tahap selanjutnya dalam tabel 9 adalah mengklasifikasikan ke-14 risiko tersebut ke dalam kategori risiko tinggi *(high)*, sedang *(medium)*, dan rendah *(low).*

Tabel 9. Pengelompokan Risiko berdasarkan Tingkatan Level

ID	**Kemungkinan Risiko**	***Likelihood***	***Impact***	***Risk Level***
R007	*Trouble Webserver*	4	5	*HIGH*
R008	Koneksi jaringan bermasalah	5	4	*HIGH*
R001	*Human Error*	4	3	*MED*
R009	Kerusakan *Hardware*	2	4	*MED*
R010	*Overheat*	3	3	*MED*
R011	Listrik Mati Secara Tiba-Tiba	4	3	*MED*
R013	*Server Down*	3	4	*MED*
R002	Penyalahgunaan Hak Akses	2	1	*LOW*
R003	*UI Design* Yang Sulit Dipahami	1	1	*LOW*
R004	Pencurian Data/Perangkat Keras	2	2	*LOW*
R005	*Cybercrime*	2	2	*LOW*
R006	*Hacking*	2	2	*LOW*
R012	*Data Corrupt*	1	2	*LOW*
R014	*Trouble Backup*	1	2	*LOW*

Dari proses evaluasi risiko ini, telah teridentifikasi 14 risiko yang sebelumnya telah diidentifikasi, dianalisis, dan diklasifikasikan berdasarkan tingkat risikonya. Dari ke-14 risiko tersebut, terdapat 2 risiko yang masuk ke dalam kategori risiko tinggi *(high)*, yakni: R007 *(Trouble Webserver)* dan R008 (Koneksi Jaringan Bermasalah). Sebanyak 5 risiko masuk ke dalam kategori risiko sedang *(medium)*, yaitu: R001 *(Human Error)*, R009 (Kerusakan *Hardware*), R010 *(Overheat)*, R011 (Listrik Mati Secara Tiba-Tiba), R013 *(Server Down)*. Di samping itu, ada 7 risiko yang termasuk dalam kategori risiko *low* (rendah), yaitu : R002 (Penyalahgunaan Hak Akses), R003 (*UI* design sulit dipahami), R004 (Pencurian data / perangkat keras), R005 *(Cybercrime)*, R006 *(Hacking)*, R012 *(Data Corrupt)*, R014 *(Trouble Backup).*

4.4. Perlakuan Risiko *(Risk Treatment)*

Setelah menyelesaikan tahap identifikasi risiko yang berkaitan dengan aset-aset dalam lingkungan situs web OPAC, langkah selanjutnya adalah melakukan proses perlakuan risiko. Pada tahap ini, tindakan risiko diambil terhadap risiko-risiko yang sudah diklasifikasikan berdasarkan tingkat risikonya. Usulan perlakuan risiko dapat ditemukan dalam tabel 10 di bawah ini

Tabel 10. Pengelompokan Risiko Berdasarkan Level dan Tindakan

ID	Kemungkinan Risiko	*Risk Level*	Tindakan Risiko
R007	*Trouble Webserver*	*HIGH*	Menyusun standar operasional prosedur (SOP) untuk mengatasi masalah pada Webserver dan memberikan pemberitahuan kepada pengguna terkait kendala Webserver
R008	Koneksi jaringan bermasalah	*HIGH*	Mengadopsi penyedia layanan (ISP) yang berbeda
R001	*Human Error*	*MED*	Melakukan training kepada User
R009	Kerusakan *Hardware*	*MED*	Melakukan asuransi untuk seluruh perangkat keras yang tersedia
R010	*Overheat*	*MED*	Menyediakan ruangan yang dilengkapi dengan sistem pendingin (AC) dan menambahkan pendingin untuk semua perangkat keras
R011	Listrik Mati Secara Tiba-Tiba	*MED*	Menyediakan unit penyalur daya tak terputus (UPS) atau generator sesuai dengan kebutuhan
R013	*Server Down*	*MED*	Melakukan pemeriksaan secara rutin pada basis data Situs Web Online Public Access
			Catalog Perpustakaan UIN Sunan Ampel Surabaya
R002	Penyalahgunaan Hak Akses	*LOW*	Menerapkan kebijakan salah satu pengguna untuk satu perangkat atau melibatkan proses konfirmasi login yang terkait dengan identitas pengguna
R003	*UI Design* Yang Sulit Dipahami	*LOW*	Memodifikasi antarmuka pengguna (*user interface*) agar menjadi lebih sederhana dan praktis dengan penggunaan ikon-ikon yang memiliki desain sederhana pada warna tertentu
R004	Pencurian Data/Perangkat Keras	*LOW*	Memasang perangkat keamanan seperti kamera pengawas (CCTV), alarm, dan sensor di seluruh ruangan
R005	*Cybercrime*	*LOW*	Menggunakan jaringan pribadi agar lebih sulit untuk disusupi oleh pihak yang tidak bertanggung jawab
R006	*Hacking*	*LOW*	Rutin mengganti kata sandi akun dan meningkatkan tingkat keamanan sistem
R012	*Data Corrupt*	*LOW*	Menggunakan situs web asli dan melakukan pencadangan data secara teratur setelah data diinputkan
R014	*Trouble Backup*	*LOW*	Menyusun standar operasional prosedur (SOP) terkait jadwal pencadangan berkala dan mengembangkan SOP untuk mengatasi masalah pencadangan (*trouble backup*)

5. KESIMPULAN

Penelitian ini menghasilkan 14 risiko potensial yang memiliki kemampuan mengganggu kinerja situs web OPAC. Dari jumlah tersebut, 2 di antaranya masuk dalam kategori risiko tinggi *(high)*, yaitu R007 *(trouble webserver)* dan R008 (koneksi jaringan bermasalah). Selanjutnya, terdapat 5 risiko dengan tingkat risiko sedang *(medium)*, termasuk R001 *(human error)*, R009 (kerusakan *hardware*), R010 *(overheat)*, R011 (listrik mati secara tiba-tiba), dan R013 *(server down)*. Selain itu, ada 7 risiko dengan tingkat risiko rendah *(low)*, yaitu R002 (penyalahgunaan hak akses), R003 (desain antarmuka sulit dipahami), R004 (pencurian data/perangkat keras), R005 (kejahatan siber), R006 *(hacking)*, R012 (data rusak), dan R014 *(trouble backup)*. Seluruh risiko ini berasal dari faktor manusia, sistem, serta infrastruktur. Staf TI perpustakaan harus mengelola dengan baik di masa depan, karena risiko seperti ini berpotensi menyebabkan masalah serius bagi situs web OPAC di Perpustakaan UIN Sunan Ampel Surabaya. Oleh karena itu, penelitian ini diharapkan dapat menjadi landasan bagi perpustakaan tersebut dalam mengembangkan Standar Operasional Prosedur (SOP) atau kebijakan untuk mengurangi potensi terjadinya risiko-risiko ini serta menjaga integritas sistem situs web OPAC di Perpustakaan UIN Sunan Ampel Surabaya.

DAFTAR PUSTAKA

[1] H. Hermin, M. Machmud, and H. Hasan, "Pemanfaatan Teknologi Informasi dalam Pengembangan Bisnis PT Pos Indonesia," vol. 3, no. 1, pp. 208–216, 2023.

[2] S. A. Atmojo, A. D. Manuputty, J. D. No, K. Sidorejo, K. Salatiga, and J. Tengah, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office," vol. 7, no. 3, pp. 546–558, 2020.

[3] P. Studi, S. Informasi, and U. Narotama, "Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1," vol. 11, no. September, pp. 125–136, 2021, doi: 10.34010/jati.v11i2.

[4] A. Manajemen and R. Menggunakan, "Smart Canteen SMA XYZ," vol. 7, no. 1, pp. 91–96, 2020, doi: 10.30865/jurikom.v7i1.1791.

[5] D. Prabowo and A. F. Wijaya, "Risk

Management Analysis on KKM LKF FTI UKSW Website Using ISO 31000 Framework," vol. 4, no. 1, pp. 65–76, 2022.

[6] R. Fahlepi, M. Fronita, E. Saputra, M. L. Hamzah, and A. Marsal, "Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000," vol. 7, no. September, pp. 663–674, 2023.

[7] G. Pamungkas, M. Bagas, and T. Atmojo, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA WEBSITE UMKM XYZ BERDASARKAN FRAMEWORK ISO 31000 ANALYSIS OF INFORMATION TECHNOLOGY RISK MANAGEMENT ON UMKM XYZ WEBSITE BASED ON ISO 31000 FRAMEWORK," vol. 4, no. 1, pp. 2–7, 2021.

[8] A. A. Herlambang, A. A. Gani, and D. D. Alvianto, "Pendekatan ISO 31000 : 2018 dalam Manajemen Risiko Teknologi Informasi pada Tracer Study Universitas Sebelas April ISO 31000 : 2018 Approach to Information Technology Risk Management in the Tracer Study at Universitas Sebelas April," no. September, pp. 5651–5660, 2024.

[9] R. P. Pangestu and A. F. Wijaya, "Analisis Manajemen Risiko Aplikasi SINTESA Pada Perpustakaan XYZ," vol. 2, no. 2, pp. 1–14, 2020.

[10] N. N. Setyaningrum *et al.*, "Penerapan iso 31000:2018 untuk manajemen risiko pada sistem informasi sekolah terpadu," no. April, pp. 31–44, 2024.