Analisis Manajemen Risiko pada Aplikasi Sistem Informasi Manajemen Sekolah Menggunakan ISO 31000:2018

Risk Management Analysis of School Management Information Systems Using ISO 31000:2018

[1]Anita Sulistiawati*, [2]Kristoko Dwi Hartomo
[1,2]Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
[1,2]Jl. Siwelut Pulutan Kidul, Kec. Sidorejo, Kel. Pulutan, Kota Salatiga, Jawa Tengah 50716, Indonesia
*e-mail: 682020053@student.uksw.edu

(***received*:** 21 July 2024, ***revised*:** 24 July 2024, ***accepted*:** 26 July 2024)

Abstrak

Sistem informasi manajemen sekolah adalah sebuah aplikasi yang dikelola bidang IT suatu Sekolah Menengah Kejuruan yang berada di Kota Salatiga. Aplikasi ini merupakan sebuah penerapan SI/TI bidang pendidikan yang dibuat dengan tujuan memudahkan proses bisnis sekolah menjadi lebih efektif dan efisien seperti kegiatan administrasi pembayaran SPP, mengelola nilai dan rapor, poin pelanggaran, absensi, dan biodata siswa yang dapat diakses guru dan siswa. Dengan kemudahan yang diberikan, tak dapat dipungkiri akan selalu muncul ancaman risiko yang datang baik secara internal maupun eksternal. Berdasarkan hal tersebut, kegiatan manajemen risiko perlu dilakukan guna meminimalisir risiko yang mungkin akan menghambat bahkan menghentikan proses bisnis sistem. Pada penelitian ini *framework* ISO 31000:2018 digunakan sebagai pedoman penilaian analisis risiko. Tahap yang digunakan dibagi menjadi tahap penilaian dan mitigasi risiko sehingga diharapkan dapat meminimalisir dan menanggulangi risiko yang ada. Tujuan dari penelitian ini adalah untuk melakukan penilaian risiko serta mitigasi risiko pada aplikasi sistem informasi manajemen sekolah menggunakan ISO 31000:2018. Hasil hari penelitian yang telah dilakukan terdapat 25 peluang risiko dengan tiga diantaranya berada pada level *high*, empat belas berada level *medium*, delapan berada pada level *low*. Dengan hasil dokumentasi manajemen risiko ini diharapkan menjadi acuan bagi pihak sekolah untuk menerapkan kebijakan baru guna meminimalisir peluang risiko.

Kata kunci: manajemen risiko, ISO 31000:2018, analisis risiko

Abstract

The school management information system (SIAHDU) is an application managed by the IT department of a Vocational High School in Salatiga City. This application is an application of SI/IT in the education sector which was created with the aim of making school business processes more effective and efficient, such as administrative activities for paying tuition fees, managing grades and report cards, violation points, attendance and student biodata that can be accessed by teachers and students. With the convenience provided, it cannot be denied that risks will always arise both internally and externally. Based on this, risk management activities need to be carried out to minimize risks that might hamper and stop the system's business processes. In this research, the ISO 31000:2018 framework is used as a risk analysis assessment guide. The stages used are divided into risk assessment and mitigation stages so that it is hoped that they can minimize and overcome existing risks. The aim of this research is to carry out risk assessments and risk mitigation in school management information system applications using ISO 31000:2018. The results of the day of research that was carried out contained 25 risk opportunities, three of which were at a high level, fourteen were at a medium level, eight were at a low level. It is hoped that the results of this risk management documentation will become a reference for schools to implement new policies to minimize risk opportunities

Keywords: *risk management, ISO 31000:2018, risk analysis*

 ISSN:2302-8149
e-ISSN:2540-9719

1 Pendahuluan

Transformasi digital diartikan sebagai proses perubahan yang memanfaatkan sumber daya digital demi mewujudkan pengalaman baru seperti efisien dan efektif dalam melakukan suatu pekerjaan [1] . Perusahaan atau suatu organisasi berlomba untuk semakin meningkatkan kualitas mereka dalam menjalankan proses bisnisnya dengan pemanfaatan teknologi informasi. Ilmu pengetahuan dan teknologi saat ini telah berkembang pesat sehingga menjadi pendorong perubahan pada bidang sosial, budaya, politik, ekonomi, hingga pendidikan. Saat ini, teknologi terus berkembang seiring perkembangan jaman tak lain seperti pada kasus pandemi yang melumpuhkan aktivitas pelajar dan mengharuskan mereka untuk tetap menjalankan sekolah di rumah. Hal ini membuat peranan teknologi sangat dibutuhkan keberadaanya. Peranan teknologi sangat dibutuhkan pada lembaga pendidikan karena memiliki fungsi yang efektif dan efisien seperti proses penyebaran informasi, kemudahan bertransaksi, kemudahan berkomunikasi [2]. Teknologi Sistem Informasi tidak serta merta hanya memberikan kemudahan bagi penggunanya, tetapi penggunaan yang tidak tepat hanya akan menyebabkan kelemahan dan memberikan ancaman kerugian baik meteriil atau non materiil.

SMK N 2 Salatiga adalah lembaga pendidikan yang telah menerapkan SI/TI dalam kegiatan penyaluran informasi. SMK N 2 memiliki aplikasi sistem informasi manajemen sekolah (SIM STENDZA) yang di dalamnya memuat website sekolah (SIKADU), sistem informasi manajemen sekolah (SIKADU), tes online, laporan PKL harian, laman Facebook, kanal youtube, Instagram, panduan aplikasi, hingga repositori alumni yang dapat di akses pada aplikasi ini. Fokus penelitian kali ini adalah pada sistem informasi manajemen sekolah (SIKADU). SMK N 2 menerapkan sistem informasi manajemen sekolah guna mempermudah warga sekolah dari siswa, hingga tenaga pengajar untuk membuat pekerjaan seperti penyebaran informasi lebih efektif dan efisien. Sistem infromasi sekolah ini dapat digunakan oleh pengajar untuk penginputan nilai, penginputan poin pelanggaran, update data siswa, penginputan absen, dan lain lain. Sistem informasi sekolah ini dikelola langsung oleh bidang IT sekolah sehingga segala pembaruan sistem dan *maintenance* hanya dikelola oleh satu pihak.

Selama penggunaannya, pihak SMK N 2 belum pernah melakukan penilaian mengenai analisis ancaman risiko pada sistem informasi manajemen sekolah dimana sistem terus berjalan dan diperbarui dengan rentan waktu tertentu yang didalamnya memuat data data penting. Permasalahan atau hambatan yang kerap kali dialami adalah *server down* sehingga membuat sistem tidak dapat diakses dalam waktu yang tidak dapat dipastikan. Padahal, siswa bisa saja sedang malaksanakan tes online dengan batas waktu yang sudah ditentukan, jika sistem tiba-tiba down atau terjadi suatu risiko akan sangat menyusahkan bagi penggunanya termasuk guru sebagai pemantau. Maka dari itu penting untuk dilakukan analisis manajemen risiko guna menangani dan meminimalisir ancaman risiko yang dapat terjadi sewaktu waktu [3] . Sebuah lembaga pendidikan penting untuk melakukan proses manajemen yang tersistematis seperti kebijakan dan prosedur, pelatihan karyawan, serta pengendalian secara berkala sebab melakukan manajemen risiko yang tepat dapat meminimalisir munculnya ancaman atau gangguan operasional yang mengancam berjalannya pelayanan pada suatu lembaga pendidikan [4] . SMK 2 harus melakukan analisis risiko yang tepat seperti penilaian risiko yang meliputi identifikasi risiko, analisis risiko, dan evaluasi risikos serta tahap perlakuan risiko atau mitigasi risiko [5] . Risiko merupakan hambatan yang disebabkan oleh penggunaan suatu proses, sedangkan manajemen risiko adalah upaya mencegah dan menanggulangi faktor kemungkinan risiko yang dapat menyebabkan hambatan suatu sistem informasi. ISO 31000:2018 merupakan standar manajemen risiko yang dikeluarkan oleh ISO yang bertujuan untuk meningkatkan suatu kinerja sistem [6] .

Penelitian ini menggunakan framework ISO 31000:2018 karena ISO memberikan panduan penerapan analisis manajemen risiko yang tersistematis dan telah diakui secara universal [7] . Penilaian menggunakan ISO 31000 dibagi menjadi tiga proses yaitu identifikasi risiko (*risk identification*), analisis risiko (*risk analys*t), dan evaluasi risiko (*risk evaluation*) serta langkah terakhir adalah perlakuan atau mitigasi risiko (*risk treatment*). Tujuan dari penelitian ini adalah ingin melakukan penilaian risiko terhadap Sistem Informasi Majamenen Sekolah yang mencakup identifikasi, analisis, evaluasi, dan juga rencana mitigasi risiko yang dapat digunakan untuk pengukuran risiko dan manajemen risiko bagi pihak sekolah. Sehingga dengan dilaksanakannya penelitian ini diharapkan dapat menghasilkan pedoman bagi pihak sekolah untuk dapat menanggulangi adanya ancaman risiko yang dapat terjadi sewaktu-waktu. Penelitian ini bermanfaat

 ISSN:2302-8149
e-ISSN:2540-9719

bagi penulis karena menggetahui faktor faktor risiko atau ancaman risiko yang bisa saja terjadi sehingga dapat menjadikan solusi atau penanggulangan risiko bagi pihak sekolah, sedangkan pihak sekolah mendapatkan data untuk memeriksa kembali sistem yang digunakan akan mengalami ancaman risiko berupa apa saja, dan mitigasi risiko apa yang harus dilakukan.

2 Tinjauan Literatur

Penelitian terdahulu telah banyak dilakukan manajemen risko dengan ISO 31000 seperti penelitian [8], [9], [10]. Penelitian pertama mengenai ISO 31000 oleh Wirawan Harefa pada tahun 2022 dengan judul "Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang". Penelitian ini berfokus pada aplikasi ERP yang membantu mengelola proses bisnis perusahaan seperti data barang keluar dan masuk, stok barang, yang terintegrasi dengan divisi lainnya. Hasil dari penelitian ini antara lain 3 risiko dengan *risk level high*, 13 risiko dengan *risk level medium*, dan 10 risiko dengan *risk level low*. Kemungkinan risiko dengan level teratas terjadi pada server down, web service mati secara tiba-tiba, dan koneksi jaringan terputus. Tindakan yang dapat dilakukan adalah dengan melakukan pemeriksaan berkala, melakukan troubleshooting, dan mengganti ISP (Internet Service Provider) dengan yang baru. Tujuan dari penelitian ini adalah meminimalisir segala kemungkinan risiko yang sedang dialami ataupun yang akan terjadi, serta memberikan rekomendasi. Sehingga dengan penelitian ini diharapkan dapat menjadi patokan bagi CV. Ribka untuk manangani dan memberikan solusi terbaik atas kemungkinan risiko yang mungkin dapat terjadi sewaktu waktu [8].

Penelitian selanjutnya dilakukan oleh Sekar Ayu Diah Pitaloka dengan judul "Penerapan ISO 31000:2018 pada Aktivitas Manajemen Risiko Aplikasi Libsys Minat Siswa" tahun 2023. peneliti melakukan analisis manajemen risiko dengan ISO 31000 pada aplikasi Libsys minat siswa, dimana aplikasi ini digunakan untuk mengetahui bakat minat siswa dan pengajar dapat memberikan arahan yang terbaik. Terdapat 17 kemungkinan risiko dengan 4 level risiko tinggi (*high*), 8 kemungkinan risiko sedang (*medium)*, dan 5 kemungkinan risiko rendah (*low*). Risiko tinggi ada pada konten tes minat siswa tidak sesuai dengan teori psikologi professional, aplikasi mengalami kendala saat pengoperasian, kerjasama dengan psikolog terputus, dan server aplikasi Libsys Minat Siswa down. Tujuan dari penelitian ini adalah menerapkan ISO 31000:2018 pada aktivitas manajemen risiko aplikasi Libsys Minat Siswa. Dari hasil penelitian ini disimpulkan penggunaan ISO 31000:2018 teruji serta memberikan panduan dalam melakukan analisis manajemen risiko pada aplikasi ini. Penelitian ini hanya melakukan analisis pada libsys minat siswa, sehingga pada penelitian selanjutnya dapat dilakukan analisis manajemen risiko pada aplikasi yang ada di perusahaan agar memiliki data manajemen risiko yang telah terdokumentasi [9] .

Penelitian juga dilakukan oleh Yeni Erlika dengan judul "Analisis IT Risk Management di Universitas Bina Darma menggunakan ISO31000" pada tahun 2020. Penelitian ini melakukan analisis risiko pada teknologi informasi yang digunakan oleh Universitas Bina Darma sebagai pendukung dalam menjalankan proses bisnisnya. Menghasilkan 20 risiko dimana 10 kemungkinan risiko berada pada level sedang, dan 10 kemungkinan risiko berada pada level rendah. Solusi atas risiko yang didapat dilakukan dengan cara mitigasi risiko dan berbagi, dalam hal ini berbagi diartikan sebagai kerjasama dalam tim. Fokus penelitian ini adalah untuk menganalisis dan mengimplementasikan IT *risk management* pada perguruan tinggi dengan ISO 31000:2018. Penelitian ini menghasilkan laporan risiko IT yang terdapat pada aplikasi yang digunakan saat ini [10].

Berdasarkan penelitian terdahulu, dapat disimpulkan bahwa setiap organisasi atau perusahaan yang memanfaatkan teknologi informasi di dalamnya pasti selalu timbul adanya risiko yang mengancam. Maka dari itu peran dilakukannya manajemen risiko sangat dibutuhkan guna mengetahui dan mempersiapkan rencana mitigasi risiko. Pada penelitian ini ISO 31000:2018 digunakan sebagai pedoman dalam melaksanakan analisis manajemen risiko pada aplikasi sistem informasi manajemen sekolah. ISO 31000:2018 merupakan standar dilakukan manajemen risiko yang diterbitkan pada 13 November 2009 oleh International Organization for Standarization [11]. ISO 31000 memiliki tahap penelitian antara lain penilaian risiko yang meliputi identifikasi risiko, analisis risiko, dan evaluasi risiko, tahap selanjutnya adalah kegiatan perlakuan atau mitigasi risiko. ISO 31000:2018 memastikan bahwa sebuah instansi memiliki sumber daya untuk melakukan manajemen risiko demi tercapainya perubahan yang efektif dan efisien, selain itu ISO 31000:2018 adalah standar untuk *universal* yang

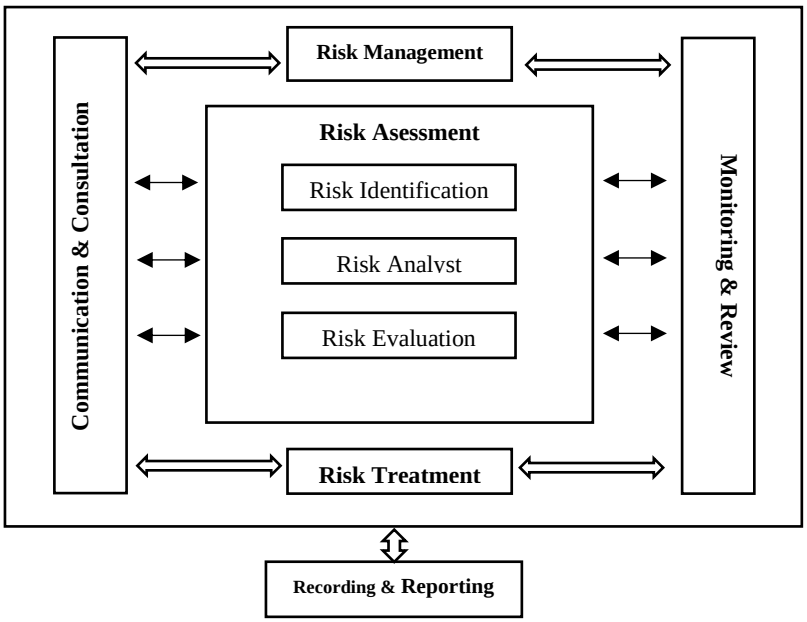
 ISSN:2302-8149
e-ISSN:2540-9719

tidak terfokus pada satu instasi tertentu [12]. Fokus pada penelitian ini adalah melakukan analisis manajemen risiko pada aplikasi sistem informasi manajemen sekolah menggunakan framework ISO 31000:2018. Perbedaan penelitian ini dengan penelitian terdahulu antara lain terletak pada analisis yang dilakukan pada aplikasi sistem informasi manajemen sekolah yang dikelola oleh Tim IT SMK N 2 Kota Salatiga. Kedua, penelitian ini dilakukan pada lembaga pendidikan tingkat SMK (Sekolah Menengah Kejuruan) dan merupakan sekolah dengan tingkat terakreditasi A dimana peluang dan ancaman risiko yang dapat terjadi pasti berbeda-beda. Terakhir, penelitian ini menghasilkan dokumentasi manajemen risiko sehingga bermanfaat bagi pihak sekolah sebagai pedoman untuk menanggulangi dan menangani ancaman risiko tanpa harus mempersiapkan dari awal.

3 Metode Penelitian

Penelitian ini dilakukan dengan pendekatan kualitatif. Metode kualitatif dapat mengetahui hal yang terjadi dan dialami pada kasus penelitian seperti perilaku, persepsi, dan juga tindakan secara langsung [13]. Data tersebut didapat dari wawancara langsung kepada divisi bagian teknologi informasi. Kegiatan atau tahap awal yang dilakukan adalah melakukan komunikasi dan konsultasi terhadap masalah yang ingin diteliti dengan staf IT yang ada di SMK N 2 yaitu Bapak Arif Basuki Wibowo, S.pd. Dengan ini peneliti memperoleh data dan fakta yang sebenarnya mengenai kasus yang akan diteliti.

Penelitian pada sistem informasi manajemen sekolah ini disajikan dengan *framework* ISO 31000:2018 dimana merupakan panduan dalam melakukan manajemen risiko yang telah diakui secara *universal*. Proses manajemen risiko merupakan monitoring dan usaha untuk menghasilkan sebuah inovasi pengendalian risiko.



Gambar 1. Tahap penelitian

Gambar 1 menyediakan proses atau alur pelaksanaan manajemen risiko. Tahap penilaian risiko terdapat tiga proses diantaranya identifikasi risiko, analisis risiko, dan evaluasi risiko [14] :

1. Identifikasi Risiko *(Risk Identification*)
   Pada penelitian ini, identifikasi risiko dilakukan dengan cara wawancara secara langsung kepada divisi IT yang bertanggung jawab. Proses identifikasi yang dilakukan mendapatkan data berupa identifikasi aset, identifikasi ancaman, identifikasi kemungkinan, dan juga identifikasi dampak [15] .
2. Analisis Risiko (*Risk Analyst*)
   Analisis risiko merupakan proses identifikasi *probability* atau faktor risiko yang mungkin terjadi, menghasilkan skala prioritas risiko yang terstruktur, setelah itu dilakukan evaluasi [16] .

Dengan dilakukan analisis risiko dapat mengukur dan menentukan suatu risiko tergolong dalam kondisi yang mana, hal ini tentu perlu dengan pertimbangan dan perhitungan yang tepat[17] .

3. Evaluasi Risiko (*Risk Evaluation)*
   Tahap evaluasi risiko adalah proses pengelompokan risiko berdasarkan kategori risiko yang terdiri atas risiko tinggi(*high*) yaitu risiko dengan tingkat kewaspadaan paling tinggi, risiko sedang(*medium*) yaitu risiko dengan tingkat menengah, risk rendah(*low*) yaitu risiko dengan tingkat rendah. Dengan ini evaluasi risiko dapat digunakan untuk penentuan tingkat dan kategori risiko [18] .

Tahap selanjutnya adalah melakukan perlakuan risiko *(risk treatment*) guna menentukan sikap yang seharusnya diberikan terhadap risiko-risiko yang terjadi dan cara ini dianggap sebagai solusi untuk meminimalisir adanya ancaman.

Metode pengumpulan data dalam penelitian ini adalah dengan cara wawancara langsung dengan divisi IT SMK N 2 Salatiga, menghasilkan informasi penting yang berkaitan seperti permasalahan yang dapat terjadi. Metode wawancara dapat mengetahui permasalahan dan informan dapat secara langsung memberikan data secara jelas dan pasti seperti identifikasi aset, risiko, dan sebagainya.

4 Hasil dan Pembahasan

Bagian ini akan menyediakan hasil dan pembahasan mengenai proses pemanfaatan ISO 31000:2018 pada aplikasi sistem informasi manajemen sekolah. Tahap pembahasan diawali identifikasi dan di akhiri dengan proses mitigasi risiko.

A. Identifikasi risiko

Proses ini menyajikan data yeng telah di identifikasi melalui observasi dan wawancara. Identifikasi risiko terdiri dari identifikasi aset, identifikasi kemungkinan risiko, dan identifikasi dampak risiko.

a) Identifikasi aset

Tahap identifikasi aset terhadap sistem informasi manajemen sekolah yang meliputi aset data, aset *software*, aset *hardware*.

Tabel 1. Identifikasi aset terhadap aplikasi sekolah

Komponen Sistem Informasi	Aset
Data	1. Menu SPP siswa 2. Menu poin pelanggaran 3. Menu biodata siswa 4. Menu nilai MID 5. Menu daftar hadir/ absensi 6. Menu rapor siswa 7. Menu update biodata
Software	Aplikasi sistem informasi manajemen sekolah
Hardware	*Personal Computer* i3 UPS (*Uninterruptible Power Suply*) Server jaringan

Tabel 1 menjelakan aset apa saja yang ada pada aplikasi manajemen sekolah berupa komponen sistem informasi aset data, aset *software*, dan aset *hardware* yang di dalamnya terdapat informasi informasi.

b) Identifikasi kemungkinan risiko

Setelah dilakukan identifikasi aset terdapat hasil dari data, *software*, dan *hardware*. Tahap selanjutnya adalah melakukan identifikasi kemungkinan risiko yang dapat dilakukan dengan pengelompokan atau penyesuaian berdasarkan faktor alam, faktor manusia, dan faktor sistem informasi.

 ISSN:2302-8149
e-ISSN:2540-9719

Tabel 2. Identifikasi kemungkinan risiko

Faktor	Kode Risiko	Kemungkinan Risiko
Alam / Lingkungan	R1	Kebakaran
	R2	Listrik padam
	R3	Gempa Bumi
	R4	Tanah Longsor
	R5	Petir
	R6	Angin Putting Beliung
Manusia	R7	Pencurian Data
	R8	*Cybercrime*
	R9	*Human error*
	R10	Kesalahan penginputan data
	R11	Penyalahgunaan hak akses
	R12	Pencurian *hardware*
	R13	Kurangnya SDM yang memadahi
	R14	Penggunaan sistem yang tidak diperbarui
Sistem informasi dan infrastruktur	R15	Jaringan terputus
	R16	Kegagalan update data
	R17	*Overload* data
	R18	Serangan virus
	R19	*Server down*
	R20	*Database error*
	R21	Sistem lambat
	R22	*overheat*
	R23	*Memory full*
	R24	Sistem ter *log out*
	R25	Kerusakan perangkat keras

Tabel 2 menyediakan faktor-faktor risiko yang dapat terjadi dari hasil wawancara kepada staff IT SMK 2 Salatiga. Terdapat 25 kemungkinan risiko yang telah dikelompokkan berdasarkan asal atau faktor yang mempengaruhinya.

c) Identifikasi dampak risiko

Tahap selanjutnya adalah identifikasi dampak risiko. Dari identifikasi risiko memperoleh beberapa risiko dari faktor alam atau lingkungan, faktor manusia, dan faktor sistem informasi dan infrastruktur. Identifikasi risiko akan menganalisis dampak apa yang dapat terjadi jika risiko-risiko tersebut terjadi.

Tabel 3. Identifikasi dampak risiko

Kode Risiko	Kemungkinan Risiko	Dampak
R1	Kebakaran	Aset berupa komputer, kabel, jaringan terputus menyebabkan proses bisnis terhenti dan instansi mengalami kerugian secara finansial.
R2	Listrik padam	Berhentinya semua sistem proses bisnis yang berjalan menggunakan jaringan listrik.
R3	Gempa Bumi	Instansni sekolah mengalami kerusakan infrastruktur.
R4	Tanah Longsor	Instasni sekolah mengalami kerusakan infrastruktur, serta terputusnya jaringan

 ISSN:2302-8149
e-ISSN:2540-9719

		kabel menyebabkan terhambatnya koneksi jaringan.
R5	Petir	Kerusakan jaringan membutuhkan perbaikan *maintenance.*
R6	Angin Puting Beliung	Koneksi internet mengalami penghambatan sebab jaringan terputus.
R7	Pencurian Data	Berpotensi data data siswa disalahgunakan untuk hal yang kurang baik oleh oknum.
R8	*Cybercrime*	Terjadi kecurangan data dan sistem pada aplikasi sekolah.
R9	*Human error*	Merugikan instansi dan menghambat kinerja proses bisnis.
R10	Kesalahan penginputan data	Kerugian bagi pemilik data dan ketidak sinkron an dengan data satu dan lain.
R11	Penyalahgunaan hak akses	Pihak yang tidak bertanggung jawab dapat menyalahgunakan data dan memanipulasi data.
R12	Pencurian *hardware*	Menyebabkan kerugian secara materiil.
R13	Kurangnya SDM yang memadahi	Sistem informasi tidak berjalan sebagaimana mestinya karena SDM kurang memahami fungsi dan paham teknologi yang ada.
R14	Penggunaan sistem yang tidak diperbarui	Siswa terhalang mendapatkan informasi terbaru karena penggunaan sistem yang tidak di update sesuai versi terbarunya
R15	Jaringan terputus	Gagal dalam melakukan akses masuk kedalam sistem, terjadi loading.
R16	Kegagalan update data	Penginputan ulang data menyita waktu lebih lama.
R17	*Overload* data	Terlalu banyak data yang ada menyebabkan sistem mengalami *delay* atau lamban
R18	Serangan virus	Komputer mengalami kerusakan karena virus menyebabkan terganggunya suatu sistem
R19	*Server down*	Terjadi kegagalan sistem menyebabkan guru dan siswa tidak bisa melakukan akses masuk
R20	*Database error*	Gagal dalam melakukan penginputan data siswa
R21	Sistem lambat	Menyebabkan sistem berhenti dan tidak dapat digunakan
R22	*overheat*	Perangkat jaringan mengalami panas secara ekstrim menyebabkan kerusakan hardware
R23	*Memory full*	Data tidak dapat tersimpan secara maksimal
R24	Sistem ter *log out*	Pencarian data ulang atau penginputan ulang data yang belum tersimpan
R25	Kerusakan perangkat keras	Kinerja sistem terganggu, diperlukannya penggantian *hardware*

Tabel 3 menjelaskan kemungkinan risiko serta dampak apa saja jika risiko tersebut terjadi.

B. Analisis risiko

Tahap analisis risiko (*Risk Analys*) merupakan tahap penentuan nilai dari tiap-tiap kemungkinan risiko. Telah didapat identifikasi risiko dan dampak yang ditimbulkan. Langkah selanjutnya adalah

 ISSN:2302-8149
e-ISSN:2540-9719

tabel kriteria *likelihood* (kemungkinan risiko) dan *impact* (dampak risiko). Di bawah ini adalah tabel 4 kriteria likelihood yang dibagi menjadi beberapa kategori risiko.

Tabel 4. *Likelihood* (kemungkinan risiko) menyajikan nilai frekuensi

Nilai	Kriteria	Keterangan	Frekuensi
1	*Rare*	Risiko yang hampir tidak terjadi	>25 bulan
2	*Unlikely*	Risiko yang jarang terjadi	13 – 24 bulan
3	*Possible*	Risiko yang terkadang terjadi	7 – 12 bulan
4	*Likely*	Risiko yang sering terjadi	4 – 6 bulan
5	*Certain*	Risiko yang pasti terjadi	1 – 3 bulan

Setelah dilakukan tahap kategori kemungkinan risiko, selanjutnya dilakukan penilaian dampak (impact) terhadap kemungkinan risiko yang terjadi. Tabel 5 penilaian dampak dibawah ini dikelompokkan berdasarkan beberapa kategori yang menggambarkan seberapa besar dampak yang ditimbulkan.

Tabel 5. Nilai *impact* (dampak risiko) tiap kriteria

Nilai	Kriteria	Keterangan
1	*Insignificant*	Risiko yang ada tidak mengganggu aktivitas proses bisnis pada instansi sekolah
2	*Minor*	Risiko yang ada sedikit mengganggu aktivitas dan proses bisnis instansi sekolah
3	*Moderate*	Risiko yang ada dapat menghambat sebagian aktivitas bisnis sekolah
4	*Major*	Risiko yang ada dapat mengganggu hampir seluruh dan menyebabkan proses bisnis terhambat
5	*Castastrophic*	Risiko yang ada dapat menghentikan aktivitas proses bisnis sekolah secara total

Tahap selanjutnya adalah penilaian kriteria *Likelihood* dan kriteria *impact* yang tersedia pada tabel 6. Tabel dibawah menjelaskan penilaian seberapa sering terjadinya suatu ancaman dan seberapa dampak yang ditimbulkan. Penilaian dibawah dapat dilihat pada tabel sebelunya mengenai pengertian tiap angka *likelihood* dan *impact*.

Tabel 6. Nilai hasil analisis kemungkinan risiko (*Likelihood)* dan dampak risiko (*Impact)* pada aplikasi sistem informasi manajemen sekolah

Kode Risiko	Kemungkinan Risiko	*Likelihood*	*Impact*
R1	Kebakaran	1	5
R2	Listrik padam	5	2
R3	Gempa Bumi	1	3
R4	Tanah Longsor	1	5
R5	Petir	2	4
R6	Angin Putting Beliung	2	2
R7	Pencurian Data	3	2
R8	*Cybercrime*	1	3
R9	*Human error*	3	3
R10	Kesalahan penginputan data	3	2
R11	Penyalahgunaan hak akses	2	1
R12	Pencurian *hardware*	1	4

R13	Kurangnya SDM yang memadahi	2	2
R14	Penggunaan sistem yang tidak diperbarui	5	3
R15	Jaringan terputus	5	4
R16	Kegagalan update data	3	2
R17	*Overload* data	2	2
R18	Serangan virus	3	4
R19	*Server down*	4	5
R20	*Database error*	2	4
R21	Sistem lambat	1	3
R22	*overheat*	3	3
R23	*Memory full*	2	2
R24	Sistem ter *log out*	2	4
R25	Kerusakan perangkat keras	2	4

Berdasarkan tabel 6, telah didapat penilaian *likelihood* dan *impact* seperti yang tertera pada tabel, penilaian tersebut akan berpengaruh pada tingkat kepentingan suatu risiko karena menentukan suatu posisi risiko berada pada tingat sedang, medium atau tinggi. Selanjutnya, dilakukan tabel evaluasi risiko.

C. Evaluasi Risiko (*Risk Evaluation*)

Berikut adalah tabel matriks evaluasi risiko yang mengelompokkan kemungkinan risiko kedalam kategori yang berdasar dari *likelihood* dan *impact.* Matriks evaluasi risiko tersusun dari kategori *low* berwarna hijau, *medium* berwarna kuning, dan *high* berwarna merah yang dapat dilihat pada tabel 7.

Tabel 7. Matriks evaluasi risiko (*risk evaluation*)

Likelihood						
	Certain	(5)			R14	R15	
	Likely	(4)					R19
	Possible	(3)		R7 R10 R16	R9 R22	R18	
	Unlikely	(2)	R11	R6 R13 R17 R23		R5 R20 R24 R25	R2
	Rare	(1)			R3 R8 R21	R12	R1 R4
			(1)	(2)	(3)	(4)	(5)
			Insifnificant	*Minor*	*Moderate*	*Major*	*Castastrophic*
					Impact		

Tabel 7 merupakan hasil pengelompokan 25 risiko kedalam matriks evaluasi risiko dengan kategori rendah, sedang, hingga tinggi. Berikut adalah penjabaran level risiko yang ada pada tabel 8.

Tabel 8. Evaluasi kemungkinan risiko berdasarkan *impact* dan *likelihood*

Kode Risiko	Kemungkinan Risiko	*Likelihood*	*Impact*	*Level* Risiko
R1	Kebakaran	1	5	Medium
R2	Listrik padam	5	2	Medium
R3	Gempa Bumi	1	3	Low
R4	Tanah Longsor	1	5	Medium
R5	Petir	2	4	Medium
R6	Angin Putting Beliung	2	2	Low
R7	Pencurian Data	3	2	Medium
R8	*Cybercrime*	1	3	Low

 ISSN:2302-8149
e-ISSN:2540-9719

R9	*Human error*	3	3	Medium
R10	Kesalahan penginputan data	3	2	Medium
R11	Penyalahgunaan hak akses	2	1	Low
R12	Pencurian *hardware*	1	4	Medium
R13	Kurangnya SDM yang memadahi	2	2	Low
R14	Penggunaan sistem yang tidak diperbarui	5	3	High
R15	Jaringan terputus	5	4	High
R16	Kegagalan update data	3	2	Medium
R17	*Overload* data	2	2	Low
R18	Serangan virus	3	4	Medium
R19	*Server down*	4	5	High
R20	*Database error*	2	4	Medium
R21	Sistem lambat	1	3	Low
R22	*overheat*	3	3	Medium
R23	*Memory full*	2	2	Low
R24	Sistem ter *log out*	2	4	Medium
R25	Kerusakan perangkat keras	2	4	Medium

Tabel 8 mengidentifikasi kategori level kemungkinan risiko yang berdasar *likelihood* dan *impact.* Terdapat 25 kemungkinan risiko yang telah dikategorikan, 3 kemungkinan risiko yaitu R14, R15, dan R19 termasuk dalam level tinggi (*high*), 14 kemungkinan risiko yaitu R1, R2, R4, R5, R7, R9, R10, R12, R16, R18, R20, R22, R24, R25 termasuk dalam level sedang (*medium*), dan 8 kemungkinan risiko yaitu R3, R6, R8, R11, R13, R17, R21, R23 termasuk dalam level rendah (*low*).

D. Risk Treatment (Perlakuan Risiko)

Tahap *Risk Treatment* (perlakuan risiko) adalah tahap pemberian perlakuan atau solusi risiko agar meminimalisir kemungkinan risiko yang terjadi sehingga dengan adanya sikap ini diharapkan dapat menjadi dampak baik bagi proses bisnis organisasi. Pada tahap sebelumnya telah didapat level risiko sehingga selanjutnya pada Risk treatment akan disusun sesuai level risiko dari *high*, *medium*, hingga *low*.

Tabel 9. Risk treatment (perlakuan risiko) berdasarkan kemungkinan risiko dan level risiko

Kode Risiko	Kemungkinan Risiko	Level Risiko	Perlakuan Risiko
R14	Penggunaan sistem yang tidak diperbarui	High	Melakukan audit kinerja pada bagian sistem informasi agar dapat berjalan sebagaimana mestinya termasuk melakukan update data sesuai jadwal
R15	Jaringan terputus	High	Menghubungi pihak IT agar permasalahan yang ada sesegera mungkin dapat di atasi
R19	*Server down*	High	Melakukan pembersihan cache secara berkala, terkadang cache menjadi suatu sebab sistem tidak bisa di akses
R1	Kebakaran	Medium	Siap sedia menanggulangi adanya kebakaran dengan Alat Pamadam Api / APAR
R2	Listrik padam	Medium	Menyediakan genset sebagai solusi jika tiba tiba listrik padam, sehingga bisa sesegera mungkin diatasi
R4	Tanah Longsor	Medium	Melakukan perbaikan jaringan yang terputus dan mengamankan barang

 ISSN:2302-8149
e-ISSN:2540-9719

R5	Petir	Medium	Memasang alat penangkal petir sebagai upaya
R7	Pencurian Data	Medium	Melakukan backup data dengan waktu berkala, meningkatkan pengamanan dan kata sandi.
R9	*Human error*	Medium	Melakukan pelatihan pada setiap karyawan baru agar menguasai bidangnya.
R10	Kesalahan penginputan data	Medium	Melakukan editing dan update ulang data
R12	Pencurian *hardware*	Medium	Melakukan pengamanan ruang atau penyimpanan hardware
R16	Kegagalan update data	Medium	Melakukan Pembersihan cache, refresh dan update ulang
R18	Serangan virus	Medium	Melakukan pemasangan antivirus ter update dan terpercaya
R20	*Database error*	Medium	Cheking penggunaan penyimpanan pada database, melakukan backup data berkala
R22	*overheat*	Medium	Meletakkan komputer pada suhu ruang yang cenderung dingin, penggantian kipas CPU
R24	Sistem ter *log out*	Medium	Melakukan cek sistem dan perbaikan sistem
R25	Kerusakan perangkat keras	Medium	Mengganti perangkat yang baru sesuai kebutuhan agar tidak mengganggu berjalannya sistem
R3	Gempa Bumi	Low	Malakukan pengamanan perangkat ke tempat yang lebeih aman
R6	Angin Puting Beliung	Low	Sesegera mungkin dilakukan pembenaran pada jaringan atau kabel yang rusak
R8	*Cybercrime*	Low	Pengamanan ganda dan melakukan backup data
R11	Penyalahgunaan hak akses	Low	Meningkatkan keamanan, membuat kebijakan mengenai penyalahgunaan
R13	Kurangnya SDM yang memadahi	Low	Melakukan perekrutan staff sesuai kriteria yang memadahi sehingga dapat menguasai sistem yang digunakan
R17	*Overload* data	Low	Menambah kapasitas penyimpanan data serta pengecekan penyimpanan secara berkala
R21	Sistem lambat	Low	Membersihkan cache penyimpanan, melakukan upgrade sistem
R23	*Memory full*	Low	Menyediakan penyimpanan yang lebih besar dan memadahi serta melakukan pengecekan penyimpanan yang terjadwal

Tabel 9 telah diperoleh solusi dari risiko yang ada dan diharapkan dapat dijadikan jalan keluar serta dapat menanggulangi adanya risiko sebelum terjadi pada aplikasi manajemen sekolah.

5 Kesimpulan

Dari hasil penelitian yang telah dilakukan, didapat bahwa *framework* ISO 31000:2018 terbukti memberikan panduan yang tersistematis dalam melakukan manajemen risiko pada aplikasi sistem informasi manajemen sekolah. Ditemukan 25 kemungkinan risiko yang berada pada level *high*, *medium*, dan *low*. 3 kemungkinan risiko berada pada level *high* diantaranya Penggunaan sistem yang

tidak diperbarui (R14), jaringan terputus (R15), dan *server down*(R19). 15 kemungkinan risiko berada pada level *medium* diantaranya kebakaran (R1), listrik padam (R2), tanah longsor (R$), petir (R5), pencurian data (R7), *human error* (R9), Kesalahan penginputan data (R10), Pencurian *hardware* (R12) , Kegagalan update data (R16), serangan virus (R18), database *error* (R20), *overheat* (R22), Sistem ter *log out* (R24), Kerusakan perangkat keras (R25). Serta 8 kemungkinan risiko berada pada level *low* diantaranya adalah gempa bumi (R3), Angin Puting Beliung (R6), *Cybercrime* (R8), Penyalahgunaan hak akses (R11), Kurangnya SDM yang memadahi (R13), *Overload* data (R17), Sistem lambat (R21), *Memory full* (R23). Penelitian ini diharapkan dapat menjadi acuan bagi SMK N 2 Salatiga untuk meminimalisir dan dapat menanggulanggi ancaman risiko yang terjadi. Dengan ini diharapkan instansi sekolah dapat menentukan kebijakan baru guna mencegah adanya munculnya risiko seperti faktor manusia dan intrastruktur.

Referensi

[1] K. Hadiono, R. Candra, and N. Santi, Menyongsong Transformasi Digital.

[2] N. Edwin Kiky Aprianto, "Peran Teknologi Informasi dan Komunikasi dalam Bisnis," *International Journal Administration, Business and Organization (IJABO)* |, vol. 2, no. 1, pp. 1–7, 2021, [Online]. Available: https://ijabo.a3i.or.id

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

[4] G. H. Tirayoh and P. Pangeran, "*Operational Risk Mitigation Based on Risk Management ISO 31000:2018-Balanced Scorecard to Increase the Income and Reputation: Case Study at IEC*."

[5] H. Yefany Syahputri and M. L. Kitri, "*Enterprise Risk Management Analysis of Group XYZ Based on ISO* 31000:2018 *Framework*," 2020. [Online]. Available: http://myjms.moe.gov.my/index.php/ajafin

[6] J. Bina Komputer, P. Studi Sistem Informasi, F. Teknologi Informasi, and U. Kristen Satya Wacana, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional."

[7] M. I. Fachrezi, A. Dwika Cahyono, and P. F. Tanaem, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga," *Jurusan Sistem Informasi*, vol. 8, no. 2, 2021, [Online]. Available: http://jurnal.mdp.ac.id

[8] W. Harefa and K. D. Hartomo, "Analisis Manajemen Risiko Dengan Menggunakan *Framework* ISO 31000:2018 Pada Sistem Informasi Gudang", [Online]. Available: http://jurnal.mdp.ac.id

[9] S. A. Diah Pitaloka and E. Maria, "SISTEMASI: Jurnal Sistem Informasi Penerapan ISO 31000:2018 pada Aktivitas Manajemen Risiko Aplikasi Libsys Minat Siswa Implementation of ISO 31000:2018 in Risk Management Activities of Libsys Application Student Interest." [Online]. Available: http://sistemasi.ftik.unisi.ac.id

[10] Y. Erlika *et al.*, "Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000".

[11] P. Kanantyo, F. S. Papilaya, K. S. Wacana, J. Blotongan, K. Salatiga, and J. Tengah, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)," 2021. [Online]. Available: http://jurnal.mdp.ac.id

[12] E. Ratter, M. Kalbarczyk, and K. Pietrzak-Wiszowaty, "The Utilization of Lean Management Tools in the Application of Risk Management Methods According to ISO 31000:2018 The Utilization of Lean Management Tools in the Application of Risk Management Methods According to ISO 31000:2018 66," 2024.

[13] R. Bisma, "Manajemen Risiko Aset Teknologi Informasi: Studi kasus Implementasi Manajemen Risiko SPBE Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan."

[14] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *Journal of Computer Science and Engineering (JCSE)*, vol. 1, no. 2, pp. 128–146, Aug. 2020, doi: 10.36596/jcse.v1i2.76.

[15] D. Kurniawan, R. Prabowo, J. Ilmu Komputer FMIPA Universitas Lampung Jalan Sumantri Brojonegoro No, and B. Lampung, "Analisis Manajemen Risiko Sistem Informasi Pengelolaan Data English Proficiency Test (EPT) dan Portal Informasi di UPT Bahasa Universitas Lampung Menggunakan Metode ISO 31000," 2020.

[16] 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. 91, Feb. 2020, doi: 10.30865/jurikom.v7i1.1791.

[17] I. Putu, A. Eka, P. #1, and T. S. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," *Jurnal Telematika*, vol. 15, no. 2.

[18] K. M. Linda Lole and E. Maria, "Analisis Manajemen Risiko Pada Aplikasi Pegadaian Digital Service Menu Tabungan Emas Menggunakan ISO 31000:2018," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 3, no. 3, p. 319, Mar. 2022, doi: 10.30865/json.v3i3.3891.