AITI: Jurnal Teknologi Informasi, Volume 23 No. 1 Maret 2026, 1-13
ISSN 1693-8348 E-ISSN 2615-7128
DOI: 10.24246/aiti.v23i1.1-13

JURNAL TEKNOLOGI INFORMASI

Analisis manajemen risiko pada *e-learning* SMAN 1 Ambarawa dengan menggunakan ISO 31000:2018

Hesni Joice Isabel Br Barus [1)]*, Andeka Rocky Tanaamah [1)], Akhmad Muttamaqin [2)]
[1)]Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo No. 1-10, Salatiga, Indonesia
[2)]SMA Negeri 1 Ambarawa
Jl. Yos Sudarso No. 46, Kupangtengah, Kec. Ambarawa, Jawa Tengah
Email: *hesniisabel@gmail.com

Riwayat Artikel

Diterima:	Direvisi:	Disetujui:
08-01-2025	11-02-2025	12-02-2025

Abstract

This study aims to identify the main risks faced by SMAN 1 Ambarawa, evaluate the extent to which these risks are currently managed, and develop strategic recommendations to overcome existing obstacles and potential future risks. The framework used in this research is ISO 31000:2018 risk management framework. This research employs a qualitative approach, particularly through interviews with relevant stakeholders, to identify and analyze the problems that may affect school operations. Through this qualitative approach, various existing and potential risks can be systematically identified and analyzed. The identified risks are then analyzed and categorized into three levels: low, medium, and high risk, based on their likelihood and impact. Furthermore, appropriate risk treatment strategies are proposed for each identified risk to minimize negative consequences and improve institutional preparedness. The results of this study provide practical recommendations for SMAN 1 Ambarawa in managing risks and in developing preventive strategies to reduce the possibility of future disruptions in school activities and management processes.

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

Abstrak

Penelitian ini bertujuan untuk mengidentifikasi risiko-risiko utama yang dihadapi oleh SMAN 1 Ambarawa, menganalisis sejauh mana risiko-risiko tersebut telah dikelola, dan menyusun rekomendasi strategis untuk mengatasi hambatan dan potensi risiko yang dapat terjadi. Kerangka kerja yang digunakan untuk mencapai tujuan tersebut adalah dengan ISO 31000:2018. Penelitian ini menggunakan metode kualitatif dengan teknik pengumpulan data melalui wawancara kepada pihak-pihak terkait untuk memperoleh pemahaman tentang permasalahan yang dihadapi. Melalui pendekatan tersebut, diperoleh berbagai risiko maupun potensi risiko yang dapat memengaruhi proses operasional dan pencapaian tujuan sekolah. Risiko-risiko yang teridentifikasi kemudian dianalisis dan diklasifikasikan ke dalam tiga tingkatan, yaitu risiko rendah, risiko sedang, dan risiko tinggi, berdasarkan tingkat kemungkinan dan dampaknya. Berdasarkan hasil analisis tersebut, direkomendasikan strategi

penanganan risiko yang sesuai untuk setiap kategori. Rekomendasi perlakuan risiko ini dapat dimanfaatkan pihak SMAN 1 Ambarawa sebagai acuan dalam meningkatkan efektivitas manajemen risiko, memperkuat tata kelola organisasi, serta mencegah terjadinya risiko serupa di masa mendatang.

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

Pendahuluan

Dalam era digitalisasi yang semakin berkembang pesat, peran sistem informasi juga sangat diperlukan pada beberapa bagian kehidupan manusia, tentu termasuk juga pada institusi pendidikan. SMAN 1 Ambarawa merupakan salah satu institusi pendidikan tersebut. SMAN 1 Ambarawa, menjadi sekolah unggulan yang berlokasi di Kecamatan Ambarawa. Sekolah ini juga sudah menerapkan beberapa teknologi informasi dalam proses belajar mengajarnya. Salah satunya yaitu menggunakan *e-learning* untuk membantu siswa dalam pembelajaran. *E-learning* ini berbasis *web* yang di dalamnya sudah terdapat data siswa, guru, alumni, serta materi yang bisa dipelajari oleh siswa dan guru. Dengan memaksimalkan perkembangan teknologi informasi dalam sekolah ataupun sebuah organisasi, maka risiko yang berpotensi juga dapat muncul, hingga dapat menghambat pencapaian dari tujuan sekolah tersebut [1].

Meski sudah memiliki *e-learning* yang sangat membantu siswa, *web* SMAN 1 Ambarawa juga terkadang memiliki kendala seperti *web* tidak dapat diakses, *server down*, serta ancaman lain seperti serangan virus yang dapat merusak atau mencuri data penting. Selain itu, kurangnya SDM dalam mengelola sistem juga menjadi tantangan tersendiri, karena pengelolaan yang kurang baik, masalah teknis bisa semakin sulit untuk diatasi. Hal ini tentu menjadi tantangan dan risiko yang dapat mengancam proses pembelajaran. Melalui penelitian ini, akan dianalisis risiko apa saja yang mungkin bisa mengancam media pembelajaran *online* atau daring yang menghambat atau bahkan menghalangi proses pembelajaran dengan menggunakan *framework* ISO 31000. Pentingnya menjaga data-data yang ada, seperti data siswa dan guru untuk terhindar dari kejahatan siber. Selain itu, privasi dan keamanan data pribadi siswa serta guru, yaitu informasi pribadi, catatan akademik, dan informasi sensitif lainnya harus dijaga dengan ketat. Memastikan keamanan data tersebut merupakan kewajiban moral dan hukum, serta mencegah penyalahgunaan informasi yang dapat merugikan individu yang bersangkutan.

Panduan yang diberikan pada ISO 31000 meliputi identifikasi risiko, evaluasi risiko, dan pengelolaan risiko yang menjadi solusi terbaik untuk menjaga sistem informasi [2]. Selain dari itu, manajemen risiko sangat penting digunakan sebagai alat untuk mengantisipasi ancaman dan mengurangi dampak risiko yang mungkin akan terjadi [3]. ISO 31000:2018 memberikan panduan yang lebih strategis dibandingkan

dengan versi ISO 31000:2009, dengan fokus lebih besar pada peran aktif manajemen risiko dan pengintegrasian manajemen risiko ke dalam struktur organisasi [4].

Penelitian mengenai analisis risiko menggunakan ISO 31000:2018 di sekolah ini belum pernah dilakukan, sehingga melalui penelitian ini, nantinya akan diidentifikasi risiko-risiko utama yang dihadapi, sejauh mana risiko-risiko tersebut dikelola, dan menyusun rekomendasi untuk mengatasi hambatan dan risiko yang terjadi pada SMAN 1 Ambarawa. Penelitian ini juga dapat membantu meningkatkan kesadaran akan risiko-risiko yang mungkin dihadapi oleh sistem informasi di sekolah. Dengan pengetahuan yang lebih luas mengenai risiko-risiko tersebut, maka tenaga kependidikan dapat mengambil keputusan yang tepat untuk mengurangi kemungkinan terjadinya masalah keamanan data atau gangguan operasional lainnya.

Telah terdapat beberapa penelitian tentang manajemen risiko menggunakan ISO 310000:2018. Pada penelitian manajemen risiko di SMPN 6 Salatiga, ditemukan sebanyak 26 risiko pada aplikasi *learning management system.* Hal ini yang menjadi penyebab proses pembelajaran di SMPN 6 Salatiga menjadi terganggu. Terdapat pula tiga kemungkinan risiko yang berada pada level tinggi, yang diantaranya sering terjadi gangguan pada layanan *web*, koneksi jaringan yang tidak stabil dan sering terputus, serta *server down*. Hal ini menyebabkan kegagalan dalam melakukan akses *server* dan aplikasi *moodle* [5]. Analisis manajemen risiko teknologi informasi juga dilakukan menggunakan ISO 31000:2018 pada penelitian lain. Terdapat satu risiko tinggi dari 26 kemungkinan risiko, yaitu aplikasi perusahaan tidak dapat diakses, sehingga penulisan berkas, memasukkan data, akses *email* tidak dapat dilakukan karena memerlukan aplikasi [6]. Penelitian lain pada aplikasi digital *service* menu emas menggunakan ISO 31000:2018, terdapat risiko tinggi yaitu kebocoran data sehingga diperlukannya kebijakan perlindungan aplikasi dan *maintenance password* secara berkala [7]. Analisis lain yang dilakukan terhadap manajemen risiko teknologi informasi pada perusahaan toko yang menghasilkan 16 risiko, terdapat satu risiko pada kategori tinggi yaitu *server down* yang menyebabkan terganggunya proses bisnis yang berjalan [8].

Penelitian lain pada Biro Teknologi dan Sistem Informasi (BTSI) UKSW menggunakan ISO 31000:2018, menghasilkan tiga risiko pada level *high* diantaranya kurangnya SDM pengelola sistem, program dadakan, serta kehilangan/pencurian data. Dengan risiko tersebut BTSI harus mulai menyusun mitigasi dari kemungkinan risiko yang ada, untuk meminimalisir dan mempersiapkan diri dari ancaman terjadinya risiko pada masa depan [9]. Setiap penelitian yang dilakukan memiliki hasil yang berbeda, tetapi memiliki hasil akhir dan tujuan yang sama yaitu untuk mencegah serta mengurangi risiko. Risiko ini bisa muncul kapan saja dan kepada siapa saja, sebab pada dasarnya risiko berkaitan dengan semua hal [10].

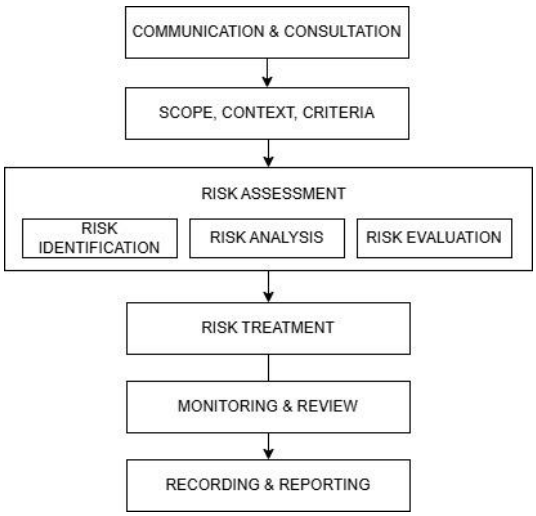
Berbagai penelitian sebelumnya, menunjukkan bahwa sistem informasi pendidikan termasuk pada *e-learning* menghadapi risiko seperti *server down,* gangguan mengakses *web,* koneksi jaringan yang tidak stabil, serta kebocoran data. Penelitian menggunakan *framework* ISO 31000:2018 telah membuktikan bahwa pendekatan ini efektif dalam mengidentifikasi, mengevaluasi, dan mengelola risiko, sehingga sejalan dengan *framework* yang digunakan pada penelitian ini. Penelitian ini akan meneliti lebih spesifik mengenai risiko pada *e-learning* di SMAN 1 Ambarawa. Selain itu, penelitian ini membantu membandingkan apakah risiko yang ditemukan dalam studi sebelumnya juga terjadi pada SMAN 1 Ambarawa atau ada faktor lainnya, sehingga pemberian rekomendasi sesuai dengan risiko yang dihadapi.

Melalui penelitian ini, akan dilakukan identifikasi dan analisis risiko yang dihadapi oleh SMAN 1 Ambarawa, serta memberikan rekomendasi untuk risiko tersebut. *Framework* ISO 31000:2018 yang diterapkan pada penelitian ini, karena memberikan pendekatan yang lebih sistematis dalam manajemen risiko dibandingkan dengan *framework* lainnya. ISO 31000:2018 memberikan panduan langkah-langkah yang lebih strategis untuk perusahaan ataupun organisasi. Selain dari itu, ISO 31000:2018 juga mudah diimplementasikan dan dapat digunakan untuk berbagai jenis bisnis. Pada konteks *e-learning, framework* ini digunakan untuk mengidentifikasi potensi risiko seperti gangguan ketika mengakses *web,* kebocoran data siswa dan guru, serta ancaman keamanan siber, sehingga sekolah dapat mengelola dan mencegah risiko tersebut. Melalui penelitian ini, SMAN 1 Ambarawa diharapkan dapat lebih peka terhadap risiko-risiko yang mungkin akan timbul sehingga dapat diatasi secara cepat dan untuk memastikan proses belajar mengajar dan operasional lainnya dapat berjalan dengan baik.

Metode Penelitian

Pengumpulan data dilakukan melalui wawancara kepada pihak terkait (guru bidang IT) untuk mengetahui permasalahan yang diteliti. Penelitian dengan metode wawancara juga disebut dengan kualitatif, yaitu menganalisis dan pemahaman yang lebih mendalam [11]. Melalui Gambar 1, dijelaskan proses tahapan yang dilakukan pada penelitian ini.

Communication and Consultation (komunikasi dan konsultasi), bagian ini bertujuan untuk memberikan gambaran dasar yang nantinya dibuat sebagai pengambilan keputusan pihak SMAN 1 Ambarawa. Komunikasi dengan pihak sekolah, yaitu guru bagian IT sebagai narasumber menjadi bagian penting dalam mengidentifikasi dan memahami risiko yang ada. Bagian ini juga bertujuan untuk mempermudah pihak-pihak yang ada dalam menganalisis risiko [12].



Gambar 1 Tahapan penelitian

Scope, Contex, Criteria (Penentuan Ruang Lingkup, Konteks, Kriteria) untuk menentukan batasan-batasan yang akan diteliti agar penilaian sesuai dengan konteks dan kriteria yang sudah ditentukan. Ruang lingkup dapat mencakup analisis risiko terhadap *e-learning, server,* jaringan, dan data yang ada.

Risk Assessment (Penilaian Risiko) pada tahapan ini, terdapat tiga proses, yaitu identifikasi risiko untuk mengetahui risiko yang dapat memengaruhi tujuan SMAN 1 Ambarawa, seperti proses pembelajaran dan operasional *e-learning.* Kedua, analisis risiko untuk menentukan tingkat potensi risiko yang muncul ataupun mungkin muncul dengan menilai potensi dampak dan kemungkinan terjadinya risiko tersebut. Terakhir yaitu evaluasi risiko, bagian ini untuk penilaian dan pengambilan keputusan dalam penanganan risiko [13].

Risk Treatment (Perlakuan Risiko) Langkah ini dilakukan untuk memastikan pilihan pengelolaan yang sesuai, untuk meminimalisir bahkan menghilangkan risiko yang dapat terjadi [14]. Berdasarkan risiko yang didapat, maka diberikan pula perlakuan risiko yang sesuai dengan yang dihadapi oleh SMAN 1 Ambarawa.

Monitoring and Review (Pemantauan dan Peninjauan) Pemantauan dan peninjauan adalah tahap pemeriksaan berkala dengan ruang lingkup yang sudah ditentukan dan dilakukan secara terus menerus untuk memastikan strategi manajemen risiko yang mungkin akan terjadi [15]. Memastikan bahwa manajemen risiko yang diterapkan efektif. Dengan melakukan pemantauan yang berkelanjutan, sekolah dapat memastikan risiko yang muncul dapat ditangani dengan cepat.

Recording and Reporting (Pencatatan dan Pelaporan) dokumentasi laporan untuk memastikan langkah manajemen risiko dalam implementasi sampai pada hasilnya. Melalui pencatatan dan pelaporan, SMAN 1 Ambarawa dapat mendokumentasikan

semua keputusan dan tindakan dalam mengatasi risiko, yang nantinya dapat digunakan sebagai referensi untuk mengelola risiko pada masa yang akan mendatang.

Hasil dan Pembahasan

Pada bagian ini dijelaskan hasil penelitian yang diperoleh berdasarkan pengumpulan data dan wawancara. Hasil penelitian ini juga memuat data yang telah dijelaskan sesuai dengan tujuan penelitian.

1. Identifikasi aset

Tabel 1 menunjukkan identifikasi aset. Aset merupakan hal penting yang dimiliki oleh perusahaan ataupun sebuah organisasi, tujuannya untuk mendukung proses bisnis dan mencapai hasil yang diinginkan. Aset pada SMAN 1 Ambarawa terbagi menjadi tiga bagian, yang pertama data, di dalamnya terdapat data siswa, data guru, data alumni, dan materi pembelajaran. Kedua, aset *software* yaitu *web* SMAN 1 Ambarawa, serta ketiga, aset *hardware* yaitu *device* (PC) dan CCTV.

Tabel 1 Komponen aset

Bagian SI/TI	Aset
Data	1. Data terdaftar siswa
	2. Data terdaftar guru
	3. Data terdaftar alumni
	4. Materi pembelajaran
Software	*Web* SMAN 1 Ambarawa
Hardware	*Device* (PC), CCTV

Tabel 2 Pemetaan risiko yang mungkin terjadi

No.	Identifikasi Risiko
R01	Bencana lingkungan
R02	Listrik Padam
R03	*Web service* tidak dapat diakses
R04	*Server down*
R05	*Server overload*
R06	Kerusakan infrastruktur
R07	Pencurian data
R08	Data dapat diakses orang yang tidak berwenang
R09	Serangan virus
R10	Data rusak
R11	*Device* siswa kurang menunjang penggunaan *software* yang dibutuhkan
R12	Kurangnya SDM pengelola sistem
R13	Kurangnya *backup* data
R14	Lambatnya adopsi teknologi baru
R15	*Human error*

2. Identifikasi kemungkinan risiko

Pada tahapan ini, identifikasi merupakan proses untuk mencari, menggali, dan mencatat risiko yang mungkin akan terjadi serta menyusun cara-cara untuk mengelola, mengurangi, dan mengantisipasi kemungkinan risiko tersebut. Kemungkinan risiko

didapat sebanyak 15 indikator yang dapat dilihat pada Tabel 2. Berdasarkan perolehan data informasi terhadap narasumber, yaitu guru pada SMAN 1 Ambarawa, dari berbagai indikator yang diwawancara, terdapat 15 indikator yang sesuai dan relevan. Bagian nomor, terdapat kode R01 - R15, huruf "R" yang berarti risiko dan angka "01" yaitu nomor urutan risiko, maka jika disebutkan R13 artinya risiko bagian nomor 13 yaitu kurangnya *backup* data. R01, R02, dan seterusnya hanyalah kode variabel yang digunakan untuk mewakili masing-masing indikator dalam analisis risiko. Kode ini tidak menunjukkan urutan tingkat risiko, melainkan hanya penamaan untuk mempermudah identifikasi setiap indikator dalam tabel.

Tabel 3 Identifikasi dampak risiko

No.	Identifikasi Risiko	Dampak
R01	Bencana lingkungan	Gangguan operasional dan kerusakan perangkat keras seperti komputer dan perangkat keras lainnya.
R02	Listrik padam	Proses bisnis yang berjalan berhenti seketika karena koneksi *wifi* mati, serta tidak dapat mengakses maupun memasukkan data ke dalam sistem.
R03	*Web service* tidak dapat diakses	Aktivitas sekolah seperti tes/ujian melalui *web* dan akses materi pembelajaran tidak bisa dilakukan, hal ini menyebabkan terganggunya proses pembelajaran.
R04	*Server down*	Banyaknya pengguna yang mengakses *web* secara bersamaan, menyebabkan gangguan layanan, seperti *web error* ataupun tidak responsif.
R05	*Server overload*	Pemasukan data tidak bisa dilakukan karena melebihi kapasitas *server.*
R06	Kerusakan infrastruktur	Aset TI mengalami kerusakan sehingga data yang belum diunggah hilang ataupun rusak.
R07	Pencurian data	Kurangnya keamanan serta privasi data sehingga terjadi masalah pada administrasi dan informasi sekolah, seperti kehilangan data dan pelanggaran privasi.
R08	Data dapat diakses orang yang tidak berwenang	Terjadi kebocoran data siswa maupun staff sekolah, maka bisa saja data dan informasi disalahgunakan
R09	Serangan virus	*Software* mengalami kerusakan, menyebabkan operasional sekolah terganggu dan data rentan dicuri.
R10	Data rusak	Kehilangan informasi bahkan gangguan operasional.
R11	*Device* siswa kurang menunjang penggunaan *software* yang dibutuhkan	Siswa tidak dapat mengikuti tes *online*, karena tidak menggunakan *device software* yang menunjang.
R12	Kurangnya SDM pengelola sistem	Kurang optimalnya pemanfaatan teknologi yang ada dan penurunan efektivitas pembelajaran.
R13	Kurangnya *backup* data	Risiko akan kehilangan data-data pada sekolah karena *backup* data yang tidak rutin.
R14	Lambatnya adopsi teknologi baru	Strategi bisnis yang kurang ataupun ketinggalan, teknologi yang ada tidak berkembang untuk memenuhi kebutuhan pemakaian siswa dan guru. Pengalaman pemakaian teknologi yang kurang baik.
R15	*Human error*	Kompetensi teknologi dan keterampilan digital yang kurang membuat pemanfaatan teknologi tidak optimal.

3. Identifikasi dampak risiko

Beberapa kemungkinan risiko dapat ditemui tidak hanya melalui *software* dan *hardware* yang sudah ada, melainkan bisa terjadi akibat lingkungan dan alam. Melalui risiko-risiko yang mungkin akan terjadi tersebut, maka diperlukannya analisis dampak yang dihasilkan. Identifikasi risiko dapat menyusun risiko-risiko yang dimiliki saat ini dan kemungkinan risiko yang mungkin dihadapi ke depannya. Pada Tabel 3 dijelaskan mengenai dampak yang disebabkan oleh risiko-risiko tersebut.

Tabel 4 menjelaskan mengenai kemungkinan frekuensi kejadian, yaitu seberapa sering kejadian tersebut terjadi. Pada bagian nilai, terdapat angka satu hingga angka lima. Angka satu merupakan nilai terendah dan sangat kecil, karena risiko yang memiliki nilai satu menunjukkan bahwa kemungkinan terjadinya sangat rendah atau bahkan tidak terjadi. Berdasarkan frekuensi kejadian, angka satu menunjukkan kemungkinan kejadian lebih dari dua tahun, yang berarti risiko dapat terjadi setelah dua tahun atau bahkan tidak terjadi sama sekali dalam rentang waktu tersebut. Singkatnya, frekuensi kejadian pada nilai angka satu mungkin saja terjadi, tetapi tidak dalam waktu dekat.

Tabel 4 Kemungkinan frekuensi kejadian

Nilai	Kategori	Keterangan	Frekuensi Kejadian
1	Sangat kecil	Risiko nyaris tidak terjadi/ kemungkinan sangat rendah terjadi	>2 tahun
2	Kecil	Risiko jarang muncul	1-2 tahun
3	Sedang	Risiko sesekali terjadi	7-12 bulan
4	Berat	Risiko sering muncul	4-6 bulan
5	Sangat Berat	Risiko hampir selalu terjadi	1-3 bulan

Tabel 5 menjelaskan tentang penilaian dampak, jika sebelumnya membahas frekuensi kejadian, maka pada Tabel 5 ini dijelaskan dampak dari risiko tersebut. Sama seperti frekuensi kejadian, penilaian dampak juga memiliki nilai dari angka satu hingga angka lima. Angka satu menunjukkan dampak paling rendah, dimana risiko tersebut tidak mempengaruhi proses bisnis. Angka dua mulai menghambat proses bisnis, hingga angka lima yang merupakan angka tertinggi. Angka lima menunjukkan bahwa dampak yang ditimbulkan oleh risiko tersebut memengaruhi seluruh proses bisnis.

Tabel 5 Penilaian dampak

Nilai	Keterangan
1	Risiko tidak mempengaruhi jalannya proses bisnis
2	Risiko sedikit menghalangi jalannya proses bisnis
3	Risiko mengganggu kelancaran proses bisnis
4	Risiko menyebabkan efektivitas proses bisnis terhambat
5	Risiko memiliki dampak besar pada seluruh proses bisnis

Setelah menentukan frekuensi kejadian dan penilaian dampak, langkah selanjutnya adalah melakukan evaluasi risiko menggunakan matriks evaluasi risiko.

Pada Tabel 6, terdapat dua aspek utama, yaitu frekuensi dan dampak. Masing-masing aspek diberi nilai berupa angka satu hingga angka lima. Pada bagian frekuensi, keterangannya terdapat pada kolom kedua dan nilai yang sesuai terdapat pada kolom berikutnya. Frekuensi dengan angka lima menunjukkan kejadian yang sangat sering terjadi. Sementara itu, pada bagian dampak, keterangannya berdasarkan baris, dimana nilai angka satu menunjukkan dampak yang sangat ringan. Matriks evaluasi risiko dapat dianalisis berdasarkan frekuensi dan dampaknya. Misalnya suatu risiko memiliki frekuensi sedang dengan angka tiga dan dampak risiko ringan dengan angka dua, maka hasil matriks evaluasi risiko menunjukkan kategori sedang.

Tabel 6 Matriks evaluasi risiko

Frekuensi	Sangat sering	5	Sedang	Sedang	Tinggi	Tinggi	Tinggi
	Sering	4	Sedang	Sedang	Sedang	Tinggi	Tinggi
	Sedang	3	Rendah	Sedang	Sedang	Sedang	Tinggi
	Jarang	2	Rendah	Rendah	Sedang	Sedang	Sedang
	Sangat jarang	1	Rendah	Rendah	Rendah	Sedang	Sedang
	Dampak		1 Sangat ringan	2 Ringan	3 Sedang	4 Besar	5 Sangat Besar

Pada Tabel 6 juga terlihat tiga jenis warna dan artinya masing-masing. Warna merah berarti risiko level tinggi (risiko pasti terjadi dan risiko tersebut dapat menghambat seluruh proses bisnis). Warna kuning berarti level risiko sedang (risiko terkadang terjadi dan risiko mengganggu proses bisnis). Terakhir, warna hijau yang berarti level risiko rendah (kemungkinan risiko terjadi kecil bahkan tidak pernah terjadi dan risiko tersebut tidak mengganggu proses bisnis). Pada masing-masing nomor di frekuensi dan dampak, frekuensi lima berarti sangat sering, sementara dampak di angka lima berarti sangat besar.

Evaluasi risiko pada Tabel 7 menunjukkan setiap level risiko yang dibuat berdasarkan frekuensi dan dampak sesuai dengan tabel matriks evaluasi risiko. Perhitungan frekuensi dibuat sesuai Tabel 4 yang menunjukkan kemungkinan frekuensi kejadian. Sementara pada bagian dampak, perhitungan dampak risiko didasarkan pada wawancara kepada narasumber sekolah. Berdasarkan evaluasi risiko tersebut, didapatkan risiko-risiko apa saja yang berada pada level tinggi, sedang, maupun rendah. Terdapat satu risiko dengan level tinggi, yaitu *web service* tidak dapat diakses. Pada level rendah terdapat dua risiko dan level sedang sebanyak 12 risiko. Melalui frekuensi, dampak, dan level tingkatan risiko, maka diberikan pula penanganan risiko yang dapat dilihat pada Tabel 8.

Tabel 7 Evaluasi risiko

No.	Identifikasi Risiko	Frekuensi	Dampak	Level
R01	Bencana lingkungan	1	3	Rendah
R02	Listrik Padam	2	4	Sedang
R03	*Web service* tidak dapat diakses	5	4	Tinggi
R04	*Server down*	2	3	Sedang
R05	*Server overload*	1	2	Rendah
R06	Kerusakan infrastruktur	2	5	Sedang
R07	Pencurian data	1	4	Sedang
R08	Data dapat diakses orang yang tidak berwenang	1	5	Sedang
R09	Serangan virus	1	5	Sedang
R10	Data rusak	2	3	Sedang
R11	*Device* siswa kurang menunjang penggunaan *software* yang dibutuhkan	2	4	Sedang
R12	Kurangnya SDM pengelola sistem	2	2	Sedang
R13	Kurangnya *backup* data	2	4	Sedang
R14	Lambatnya adopsi teknologi baru	3	2	Sedang
R15	*Human error*	3	3	Sedang

Berdasarkan penelitian dan observasi yang dilakukan, sistem informasi yang ada pada SMAN 1 Ambarawa sudah cukup baik. Hanya saja *web* yang terkadang tidak dapat diakses menjadi salah satu hambatan yang cukup mencolok. Namun meski demikian, masalah tersebut dapat diatasi dengan baik dan responsif oleh pihak sekolah, sehingga *web* tetap dapat berjalan dengan baik. Berdasarkan wawancara dengan guru bidang IT pada SMAN 1 Ambarawa sebagai narasumber, ketika terjadi masalah pada *web,* pihak sekolah langsung menghubungi kantor pusat (*Schoolmedia*) dan dari pusat memberikan respon cepat untuk dapat menyelesaikan masalah ini.

Selain dari itu, dalam meningkatkan keamanan dan mencegah risiko yang mungkin akan terjadi, pihak sekolah dapat memberikan saran kepada pengguna. Misalnya seperti, setiap pengguna menggunakan kata sandi kuat, tidak memberikan info *login* kepada orang lain, serta mengakses *web* melalui perangkat yang aman dan jaringan yang terpercaya. Pihak sekolah juga dapat memberikan edukasi mengenai keamanan data, serta dapat melakukan pelatihan yang mendasar untuk mengenali ancaman siber. Dengan demikian, pihak sekolah diharapkan dapat meminimalisir risiko dan sistem informasi pada sekolah dapat berjalan dengan baik.

Simpulan

Simpulan, sesuai dengan penelitian yang telah dilakukan, terdapat beberapa risiko dan kemungkinan risiko. Terdapat tiga tingkatan risiko, yaitu tinggi, sedang, dan rendah. Terdapat satu risiko tinggi yaitu pada R03. Pada risiko sedang terdapat 12 risiko yaitu, R02, R04, R06, R07, R08, R09, R10, R11, R12, R13, R14, R15 dan dua risiko rendah yaitu R01 dan R05.

Tabel 8 Penanganan risiko

No.	Identifikasi Risiko	Level	Perlakuan Risiko
R01	Bencana alam	Rendah	Memonitoring internet jika terjadi bencana alam yang mengganggu internet ataupun merusak internet.
R02	Listrik padam	Sedang	Menyediakan *genset* dan *Uninterruptible Power Supply (UPS).*
R03	*Web service* tidak dapat diakses	Tinggi	Melapor kepada kantor pusat (*Schoolmedia*) untuk pengecekan lebih lanjut dan melakukan pemeriksaan secara berkala.
R04	*Server down*	Sedang	Pengecekan *log server,* pemeriksaan keamanan ataupun audit keamanan, dan memeriksa koneksi jaringan.
R05	*Server overload*	Rendah	Implementasi *caching* dan menggunakan *CDN (Content Delivery Network),* menambah *RAM, CPU*, dan *bandwidth* untuk mengurangi beban *server*.
R06	Kerusakan infrastruktur	Sedang	Melakukan perawatan secara berkala terhadap infrastruktur fisik dan *backup* data secara rutin.
R07	Pencurian data	Sedang	Membatasi hak akses, menerapkan *Multi-Faktor MFA* untuk meningkatkan keamanan sistem, menggunakan *firewall* untuk memantau pergerakan jaringan.
R08	Data dapat diakses orang yang tidak berwenang	Sedang	Memberikan keamanan data yang aman dengan melakukan enkripsi, menggunakan VPN untuk mengamankan koneksi.
R09	Serangan virus	Sedang	Mengunduh antivirus pada *device* untuk mencegah virus masuk, pindai lampiran yang akan dibuka.
R10	Data rusak	Sedang	Melakukan *backup* data secara terjadwal dan pemeliharaan perangkat keras secara rutin.
R11	*Device* siswa kurang menunjang penggunaan *software* yang dibutuhkan	Sedang	Memperbaharui perangkat sekolah dan optimasi *web* agar dapat dibuka dan digunakan dengan baik.
R12	Kurangnya SDM pengelola sistem	Sedang	Melakukan pelatihan untuk SDM, melakukan perekrutan karyawan baru sesuai dengan kebutuhan.
R13	Kurangnya *backup* data	Sedang	Melakukan *backup* di beberapa lokasi seperti lokal *server cloud* secara rutin.
R14	Lambatnya adopsi teknologi baru	Sedang	Melakukan pelatihan untuk SDM terkait teknologi yang paling relevan dengan yang dibutuhkan.
R15	*Human error*	Sedang	Melakukan pengembangan keterampilan dengan *training* kepada SDM.

Risiko tinggi R03 merupakan *web service* tidak dapat diakses. Perlakuan risiko yang diberikan yaitu melapor kepada kantor pusat (*Schoolmedia*) agar dapat melakukan pengecekan lebih lanjut terhadap *web*, serta melaksanakan pemeriksaan

secara rutin guna memastikan setiap bagian operasional berjalan sesuai dengan standar dan kebijakan yang berlaku. Melalui 15 risiko dan kemungkinan risiko yang sudah dijelaskan di atas, maka sudah diberikan perlakuan risiko untuk dapat dipakai oleh SMAN 1 Ambarawa dalam mengatasi ataupun membantu risiko tidak terjadi lagi. Saran untuk penelitian selanjutnya, untuk dapat menganalisis lebih mendalam mengenai faktor-faktor penyebab risiko tinggi, seperti R03, risiko sedang, serta risiko rendah yang telah didapat. Penelitian juga dapat menganalisis dampak setiap risiko dengan lebih luas dan lengkap.

Daftar Pustaka

[1] W. Harefa, "Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 1, pp. 407–420, 2022, doi: 10.35957/jatisi.v9i1.1478.

[2] L. Febriyanti, M. Febrinazahra, Kraugusteeliana, and I. G. S. Masdiyasa, "Manajemen Risiko Sistem Informasi Unit Organisasi BPIW Kementerian PUPR Menggunakan Framework ISO 31000:2018," *J. Sist. Inf. dan Apl.*, vol. 1, no. 1, pp. 50–64, 2023, [Online]. Available: https://ejournal.upnvj.ac.id/jsia/article/view/5907

[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, 2023, doi: 10.35970/infotekmesin.v14i2.1877.

[4] A. Y. Wicaksono, "Applying ISO:31000:2018 as Risk Management Strategy on Heavy Machinery Vehicle Division," *Int. J. Sci. Eng. Inf. Technol.*, vol. 4, no. 2, pp. 198–202, 2020, [Online]. Available: https://journal.trunojoyo.ac.id/ijseit

[5] P. Kanantyo and F. S. Papilaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 4, pp. 1896–1908, 2021, doi: 10.35957/jatisi.v8i4.1082.

[6] D. Liko Ivander and F. S. Papilaya, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2018," *Kaji. Ilm. Inform. dan Komput.*, vol. 4, no. 2, pp. 1042–1051, 2023, doi: 10.30865/klik.v4i2.1174.

[7] K. M. Linda Lole and E. Maria, "Analisis Manajemen Risiko Pada Aplikasi Pegadaian Digital Service Menu Tabungan Emas Menggunakan ISO 31000:2018," *J. Sist. Komput. dan Inform.*, vol. 3, no. 3, p. 319, 2022, doi: 10.30865/json.v3i3.3891.

[8] J. N. Utamajaya, Afrina, and A. N. Fitriah, "Analisis Manajemen Risiko Teknologi Informasi Pada Perusahaan Toko Ujung Pandang Grosir Penajam

Paser Utara Menggunakan Framework Iso 31000:2018," *Sebatik*, vol. 25, no. 2, pp. 326–334, 2021, doi: 10.46984/sebatik.v25i2.1430.

[9] V. P. P. Wijaya and A. David Manuputty, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1295–1307, 2022, doi: 10.35957/jatisi.v9i2.2087.

[10] D. Stiadi, S. Jikrillah, and M. Ziyad, "Analisis Manajemen Risiko Terhadap Keberlangsungan Usaha UMKM Di Kota Banjarmasin," *J. Wawasan Manaj.*, vol. 9, no. 2, pp. 134–141, 2021.

[11] Ardiansyah, Risnita, and M. S. Jailani, "Teknik Pengumpulan Data Dan Instrumen Penelitian Ilmiah Pendidikan Pada Pendekatan Kualitatif dan Kuantitatif," *J. IHSAN J. Pendidik. Islam*, vol. 1, no. 2, pp. 1–9, 2023, doi: 10.61104/ihsan.v1i2.57.

[12] I. P. A. E. Pratama and M. T. S. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," *J. Telemat.*, vol. 15, no. 2, pp. 63–70, 2021, doi: 10.61769/telematika.v15i2.333.

[13] M. Ayuningtyas and P. F. Tanaem, "Information Technology Asset Security Risk Management at the Secretariat of the Salatiga City DPRD Using ISO 31000," *J. Inf. Syst. Informatics*, vol. 4, no. 1, pp. 92–105, 2022, doi: 10.51519/journalisi.v4i1.225.

[14] E. Muryanti and K. D. Hartomo, "Analisis Risiko Teknologi Informasi Aplikasi CATTER PDAM Kota Salatiga Menggunakan ISO 31000," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 3, pp. 1265–1277, 2021, doi: 10.35957/jatisi.v8i3.948.

[15] N. Fanny and A. Soviani, "Analisis Manajemen Risiko Di Ruang Filling RSUD dr Soedirman Mangun Sumarso Wonogiri Tahun 2020," *Infokes*, vol. 10, no. 2, pp. 12–19, 2020.