Jurnal Pendidikan Teknologi Informasi (JUKANTI)
Volume (7) No (1) April 2024–eISSN : 2621-1467

PENERAPAN ISO 31000:2018 UNTUK MANAJEMEN RISIKO PADA SISTEM INFORMASI SEKOLAH TERPADU

Nola Novita Setyaningrum[a], Evi Maria[b]

[ab]*Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Jawa Tengah*

[a] 682020044@student.uksw.edu, [b]evi.maria@uksw.edu

ABSTRAK

Tujuan riset ini adalah menerapkan standar ISO 31000:2018 untuk proses manajemen risiko pada sistem informasi sekolah terpadu (SIKADU) di SMKN 2 Salatiga. SIKADU merupakan sistem yang digunakan untuk pelayanan administrasi dan akademik sekolah. Penggunaan SIKADU tidak hanya memberikan manfaat tetapi juga memiliki potensi risiko yang merugikan, oleh karena itu perlu dilakukan pengelolaan risiko. ISO 31000:2018 dipilih sebagai *framework* untuk manajemen risiko, karena memiliki panduan yang terstruktur dan sistematis. Manajemen risiko menggunakan ISO 31000:2018 dimulai dari tahapan komunikasi dan konsultasi, penetapan konteks, penilaian risiko yang terdiri dari identifikasi risiko, analisis risiko, evaluasi risiko, dan perlakuan risiko. Hasil riset menemukan 22 kemungkinan risiko yang terjadi pada saat menggunakan SIKADU. 22 kemungkinan risiko terdiri dari dua risiko di *level high*, sebelas risiko di *level medium*, dan sembilan risiko di *level low*. Riset ini menjadi tambahan bukti bahwa ISO 31000:2018 dapat diterapkan untuk manajemen risiko sistem informasi di lembaga pendidikan. Selain itu, riset ini juga memberikan rekomendasi perlakuan risiko pada SIKADU serta dokumentasi proses manajemen risiko agar dapat digunakan SMKN 2 Salatiga sebagai acuan untuk mengelola risiko.

Kata kunci: ISO 31000:2018, Manajemen Risiko, Sistem Informasi Sekolah Terpadu

ABSTRACT

This research aims to apply the ISO 31000:2018 standard for the risk management process in the integrated school information system (SIKADU) at SMKN 2 Salatiga. SIKADU is a system used for school administrative and academic services. The use of SIKADU not only provides benefits but also has potential adverse risks, therefore risk management is necessary. ISO 31000:2018 was chosen as the risk management framework because it has structured and systematic guidelines. Risk management using ISO 31000:2018 starts from the communication and consultation stages, establishing context, risk assessment consisting of risk identification, analysis, evaluation and treatment. The research results found 22 possible risks that occur when using SIKADU. The 22 possible risks consist of two risks at the high level, eleven at the medium level, and nine at the low level. This research proves that ISO 31000:2018 can be applied to information system risk management in educational institutions. Apart from that, this research also provides recommendations for risk treatment at SIKADU and documentation of the risk management process so that it can be used by SMKN 2 Salatiga as a reference for managing risk.

Keywords: *Integrated School Information Systems, ISO 31000:2018, Risk Management*

1. PENDAHULUAN

Tak hanya organisasi bisnis dan instansi pemerintahan, lembaga pendidikan juga dituntut untuk mengimplementasikan teknologi informasi dalam seluruh proses bisnisnya [1]. Tujuannya, untuk membantu mempermudah dan mempercepat pelayanan administrasi maupun meningkatkan kualitas belajar mengajar [2]. Penggunaan teknologi informasi di lembaga pendidikan semakin meningkat saat pandemi karena kebijakan pembelajaran secara *daring* [3]. Oleh sebab itu, lembaga pendidikan tak terkecuali SMK Negeri (SMKN) 2, Salatiga memerlukan infrastruktur teknologi informasi yang memadai untuk menunjang proses bisnisnya.

SMKN 2, Salatiga adalah Sekolah Menengah Kejuruan yang pada tahun ajaran 2022/2023 memiliki 2000 siswa aktif dan 135 tenaga pengajar aktif. Ada sembilan kompetensi keahlian atau jurusan pada SMK ini. SMKN 2 Salatiga telah menggunakan sistem informasi sekolah terpadu (SIKADU). SIKADU merupakan sistem yang diciptakan oleh waka kurikulum pada tahun 2012 dan kemudian dikelola oleh Tim IT SMKN 2 Salatiga. Sistem ini digunakan siswa, guru serta karyawan untuk mengelola raport, data siswa, data kepegawaian, data mutasi, data prestasi, surat menyurat, data alumni, data poin pelanggaran, dan penilaian kinerja guru. Server SIKADU dipasang dalam jaringan lokal sekolah dan dapat diakses secara *online*. SIKADU telah terintegrasi dengan sistem informasi manajemen sekolah (SIAHDU).

Implementasi SIKADU tentunya tidak hanya memberikan manfaat bagi sekolah dan siswa tetapi juga memiliki potensi terjadinya risiko yang merugikan, jika tidak dilakukan kegiatan pengelolaan risiko. Ini karena seluruh pelayanan administrasi dan akademik sekolah sepenuhnya bergantung pada SIKADU. Kegiatan pengelolan ini dikenal dengan istilah manajemen risiko, yaitu tahapan identifikasi, penilaian, serta mencari solusi untuk mengendalikan risiko terhadap sumber daya yang tersedia [4],[5],[6],[7],[8]. Hasil wawancara dengan Tim IT ditemukan bahwa sekolah belum pernah melakukan manajemen risiko pada SIKADU, padahal Tim IT sekolah sering mendapatkan keluhan dari guru bahwa SIKADU tidak berjalan optimal. Guru juga menemukan bahwa fungsi fitur pada pengelolaan nilai masih memiliki kekurangan. Sistem belum memiliki standar arti dari nilai guru untuk setiap kompetensi mata pelajaran. Ini membuat guru memerlukan waktu lebih lama untuk mengisi keterangan penilaian kompetensi siswa karena harus menginputkan satu persatu dalam sistem. Tak hanya itu, SIKADU juga pernah tidak dapat di akses karena *Internet Service Provider* (ISP) berganti secara otomatis yang disebabkan perubahan kebijakan *Internet Service Provider* (ISP), sehingga aktivitas administrasi akademik di sekolah juga ikut terhambat dan informasi yang dihasilkan sistem tersaji tidak tepat waktu. Oleh sebab itu, kegiatan manajemen risiko untuk aplikasi SIKADU perlu dilakukan oleh SMKN 2 Salatiga.

Riset terdahulu tentang manajemen risiko teknologi informasi di lembaga pendidikan, baik itu sekolah maupun perguruan tinggi sudah dilakukan, seperti riset [9],[10],[11],[12],[13],[14]. Riset-riset tersebut menganalisis risiko pada berbagai sistem informasi baik di sekolah maupun di perguruan tinggi menggunakan standar ISO 31000:2018 untuk aktivitas manajemen risiko, seperti pada *learning management system* SMPN 6 Salatiga [9], *smart canteen* SMA XYZ [10], TI di BTSI Universitas Kristen Satya Wacana [11], sistem informasi

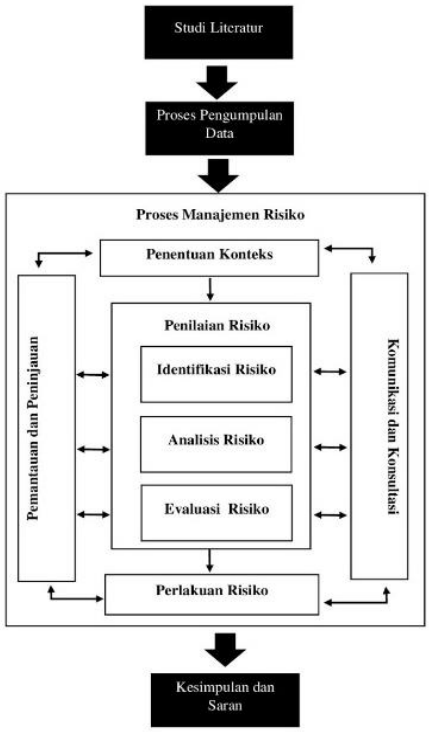
ujian secara *daring* di Sekolah Tinggi Manajemen Asuransi Trisakti [12], sistem informasi akademik di Sekolah Tinggi Teknologi Pekanbaru [13], TI di Universitas Bina Darma [14]. Hasil riset terdahulu menemukan bukti bahwa standar ISO 31000:2018 terbukti efektif untuk digunakan sebagai panduan untuk melakukan aktivitas pengelolaan risiko secara terstruktur dan sistematis dengan mempertimbangkan dasar manajemen risiko [7],[15],[16].

Dari pemetaan riset terdahulu ditemukan bahwa belum ada riset tentang aktivitas manajemen risiko pada sistem pelayanan administrasi dan akademik untuk sekolah menengah kejuruan, khususnya di SMKN 2 Salatiga. Temuan pemetaan ini sejalan dengan hasil wawancara dengan Tim IT sekolah, bahwa selama penerapan SIKADU, sekolah belum pernah melakukan kegiatan manajemen risiko. Riset terdahulu tentang SIKADU di SMKN 2 Salatiga hanya fokus melakukan analisis paket data pada jalur komunikasi SSL [17]. Hasil riset merekomendasikan server SIKADU perlu mengamankan komunikasi *client* dan *server* menggunakan SSL agar paket data dapat terenkripsi. Riset [18] merekomendasikan SMKN 2 Salatiga untuk menyusun perencanaan strategis SI/TI dalam rangka meningkatkan daya saing. Riset [19] melakukan sosialisasi *Cyber Security Awareness* pada siswa SMKN 2 Salatiga. Siswa perlu bijak ketika menggunakan media sosial, khususnya tentang keamanan data pribadi. Oleh sebab itu, tujuan riset ini adalah untuk menerapkan standar ISO 31000:2018 dalam kegiatan manajemen risiko pada SIKADU di SMKN 2 Salatiga. Hasil riset diharapkan dapat menambah bukti keefektifan standar ISO 31000:2018 dalam kegiatan pengelolaan risiko SI/TI di lembaga pendidikan, khususnya di Sekolah Menengah Kejuruan. Selain itu, hasil riset ini memberikan gambaran kondisi risiko dalam SIKADU dan memberikan rekomendasi perlakuan risiko dari penerapan SIKADU di di SMKN 2 Salatiga.

2. METODE PENELITIAN

2.1 Tahapan Penelitian

Metode kualitatif digunakan dalam riset ini untuk memperoleh pemahaman dan informasi baru dengan cara melakukan interaksi langsung dengan sumber data [20] tentang kemungkinan risiko pada sistem informasi sekolah terpadu (SIKADU) di SMKN 2 Salatiga. Data riset diperoleh dengan cara melakukan observasi dan wawancara. Tahapan riset disajikan pada Gambar 1.



Gambar 1. Tahapan Riset

Kegiatan dalam setiap tahapan riset dijelaskan berikut ini.

1. Studi literatur, dengan cara melakukan pemetaan artikel terdahulu yang membahas topik serupa untuk menambah pemahaman tentang

manajemen risiko khususnya di lembaga pendidikan. Selain itu juga dilakukan dengan cara membaca standar ISO 31000:2018 untuk menambah pemahaman ketika melakukan aktivitas manajemen risiko.

2. Pengumpulan data dengan cara melakukan observasi secara langsung pada SIKADU dan melakukan wawancara dengan Tim IT SMKN 2 Salatiga tentang proses bisnis yang diakomodasi dalam SIKADU di sana.
3. Manajemen risiko dengan menerapkan standar ISO 31000:2018 dengan lima aktivitas. Pertama, komunikasi dan konsultasi, yaitu tahap menyamakan persepsi tentang risiko dan aktivitas manajemen risiko dengan pihak sekolah (Kepala Sekolah, Guru, dan Tim IT). Kedua, penentuan konteks dengan cara menetapkan ruang lingkup dari kegiatan manajemen risiko, yaitu sistem informasi sekolah terpadu (SIKADU) SMKN 2 Salatiga dan menetapkan kriteria yang akan digunakan dalam penilaian risiko. Ketiga, penilaian risiko dimulai dari aktivitas identifikasi, analisis, dan evaluasi risiko dari SIKADU. Keempat, perlakuan risiko dengan cara memberikan masukan atau solusi untuk mengatasi risiko yang terjadi dalam SIKADU. Kelima, pemantauan dan peninjauan dengan melibatkan Tim IT SMKN 2 Salatiga untuk melakukan pengamatan terhadap implementasi dari hasil manajemen risiko.
4. Kesimpulan dan saran adalah tahap akhir riset. Bagian ini menyajikan kesimpulan riset berupa hasil kegiatan manajemen risiko terhadap SIKADU dan rekomendasi mitigasi risiko.

2.2. Standar ISO 31000:2018

Risiko adalah ketidakpastian yang dapat mengakibatkan kerugian [5],[6] dan menjadi tantangan bagi organisasi khususnya sekolah untuk mencapai tujuan. Kondisi ini mendorong dilakukannya manajemen risiko. Tujuan manajemen risiko adalah untuk mengelola risiko sehingga memperoleh hasil yang optimal [9],[21]. Penilaian risiko menjadi bagian penting dalam manajemen risiko yang memiliki tiga tahapan inti, yaitu identifikasi, analisis, dan evaluasi [4]. Riset ini menggunakan ISO 31000:2018 sebagai *framework* untuk manajemen risiko. ISO 31000:2018 diciptakan oleh *International Organization for Standardization* sebagai standar atau panduan untuk melakukan manajemen risiko [7],[15]. ISO 31000:2018 menjadi versi baru dari ISO 31000:2009 namun tetap mempertahankan tiga unsur penting dalam manajemen risiko yaitu prinsip, kerangka kerja, dan proses [22]. Tidak ada perubahan yang signifikan hanya saja standar ini merupakan bentuk sederhana dari versi lama.

3. HASIL DAN PEMBAHASAN

Hasil manajemen risiko pada sistem informasi sekolah terpadu (SIKADU) di SMKN 2 Salatiga sesuai standar ISO 31000:2018 sebagai *framework* akan dipaparkan pada bagian ini.

Komunikasi dan Konsultasi

Komunikasi dan konsultasi dilakukan bersama Kepala Sekolah dan Tim IT SMKN 2 Salatiga. Tujuannya adalah untuk menyamakan pemahaman tentang risiko dan manajemen risiko, membantu dalam pengambilan keputusan, serta menentukan cara mengatasi risiko. Selain itu dari komunikasi dan konsultasi juga didapatkan pemahaman terkait kondisi sekolah dan sistem saat ini, mengetahui

masalah terkait dengan implementasi teknologi informasi (TI)/ sistem informasi (SI) yang pernah terjadi serta cara penanganan masalah TI/SI di sana.

Penentuan Konteks

Penentuan konteks memiliki tujuan agar penilaian risiko dan perlakuan risiko terfokus hanya pada ruang lingkup serta berdasarkan kriteria risiko yang telah ditentukan. Ruang lingkup pelaksanaan manajemen risiko adalah sistem informasi sekolah terpadu (SIKADU). Adapun kriteria yang ditetapkan, yaitu kriteria *likelihood* dan kriteria *impact*. Kriteria *likelihood* digunakan untuk menilai risiko dari frekuensi waktu terjadinya risiko. Ada lima kriteria *likelihood*. yaitu *certain*, *likely*, *possible*, *unlike*, dan *rare*, seperti yang tersaji pada Tabel 1. Sedangkan, kriteria *impact* dan kerugian akibat risiko disajikan pada Tabel 2 dan Tabel 3. Ada lima kriteria *impact*, yaitu *major*, *high*, *moderate*, *minor*, dan *insignificant* untuk menilai risiko berdasarkan dampak/pengaruhnya bagi sekolah. Sedangkan, kerugian akibat risiko terbagi dalam tiga kategori yaitu *low*, *medium*, dan *high* merupakan kisaran kerugian finansial dari dampak risiko yang terjadi.

Tabel 1. Kriteria *Likelihood*

Kriteria	Keterangan Risiko	Nilai	Frekuensi
Certain	Pasti terjadi	5	1-3 bulan
Likely	Sering terjadi	4	4-6 bulan
Possible	Cukup sering terjadi	3	7-11 bulan
Unlike	Jarang terjadi	2	1-2 tahun
Rare	Hampir tidak pernah terjadi	1	>2 tahun

Tabel 2. Kriteria *Impact*

Kriteria	Nilai	Keterangan
Major	5	Risiko membuat aktivitas sekolah berhenti total.
High	4	Risiko menghambat hampir seluruh aktivitas sekolah.
Moderate	3	Risiko mengakibatkan sebagian aktivitas terganggu.
Minor	2	Risiko membuat aktivitas sekolah terhambat, namun tidak mengganggu aktivitas utama sekolah.
Insignificant	1	Risiko tidak mengganggu aktivitas sekolah.

Tabel 3. Kerugian Akibat Risiko

Kategori	Dampak Kerugian
Low	< Rp 10 Juta
Medium	Rp 10 Juta - Rp 25 Juta
High	> Rp 25 Juta

Penilaian risiko

Penilaian risiko melalui tiga tahapan penting yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko [21]. Sebelum melakukan identifikasi risiko maka perlu dilakukan identifikasi aset yang berhubungan dengan sistem informasi sekolah terpadu (SIKADU). Hasil wawancara dan observasi ditemukan tiga kategori aset. Pertama, aset data terdiri dari data raport, data siswa, data kepegawaian, data mutasi, data prestasi, data surat, data alumni, data poin pelanggaran, dan data penilaian kinerja guru. Kedua, aset *software*, yaitu sistem informasi sekolah terpadu (SIKADU). Ketiga, aset *hardware* terdiri dari *server*, komputer, wifi, *router*, *switch*, dan kabel LAN.

Setelah melakukan identifikasi aset maka dapat dilanjutkan dengan identifikasi

risiko terhadap SIKADU. Hasil identifikasi risiko dan analisisnya disajikan pada Tabel 4. Ada 22 kemungkinan risiko beserta dampak risiko yang muncul dalam implementasi SIKADU. Analisis risiko dilakukan untuk mengukur atau menilai tingkatan risiko berdasarkan frekuensi risiko dan dampak risiko bagi sekolah dengan memanfaatkan dua kriteria yang telah ditentukan pada saat penentuan konteks.

Tabel 4. Identifikasi dan Analisis Risiko SIKADU

Alur	Kemungkinan Risiko	Kode Risiko	Dampak Risiko	*Likelihood*	*Impact*
Login sistem informasi sekolah terpadu (SIKADU)	Penyalahgunaan hak akses SIKADU.	R01	Terjadi pencurian data yang dapat merugikan siswa, guru maupun karyawan dan terjadi manipulasi data.	1	3
	Pembobolan sistem pada saat login dikarenakan tidak ada batas maksimal kesalahan *input username* dan *password*.	R02	Data yang bersifat rahasia tersebar, terjadi manipulasi data.	1	3
	Username dan *password* berdasarkan Nomor Induk Siswa (NIS) dan tanggal lahir mudah diketahui oleh pihak lain.	R03	Pihak yang tidak bertanggung jawab dapat mengakses data pribadi.	4	3
Pengelolaan data raport, data siswa, data kepegawaian, data mutasi, data prestasi, surat menyurat, data alumni, data poin pelanggaran, dan penilaian kinerja guru	Tim IT kurang memahami permasalahan yang terjadi pada SIKADU.	R04	Tim IT tidak dapat mengatasi permasalahan yang terjadi pada SIKADU.	2	4
	Fitur atau konten pada SIKADU sudah tidak relevan.	R05	Pengguna SIKADU merasa kesulitan dalam berinteraksi dan memperlambat navigasi.	2	1
	Guru mata pelajaran terlambat menginputkan nilai.	R06	Raport siswa tidak dapat dicetak dan siswa tidak dapat melihat nilai melalui SIKADU.	3	2
	Kesalahan penginputan data pada SIKADU.	R07	Data yang diinputkan tidak valid, sehingga menghambat proses administrasi akademik dan merugikan siswa, guru, maupun karyawan.	3	3

Nilai raport masih dapat diedit meskipun sudah di *print*.	R08	Terjadi manipulasi data menyebabkan nilai yang ditampilkan pada sistem tidak sama dengan nilai yang sudah dicetak.	3	2
Grafik poin pelanggaran dan grafik nilai yang ditampilkan pada SIKADU tidak sesuai dengan data yang diinputkan.	R09	Informasi yang disajikan oleh SIKADU menjadi tidak akurat dan tidak dapat diandalkan.	2	2
Berkas surat, berkas penunjang data guru dan dokumentasi lomba tidak dapat diunggah ke SIKADU.	R10	Tidak ada file pendukung atau bukti pada data yang telah diinputkan, data tidak dapat disimpan.	3	2
Koneksi jaringan yang tidak stabil.	R11	Proses penginputan data memerlukan waktu yang cukup lama sehingga aktivitas administrasi dan akademik terganggu.	4	4
SIKADU mengalami *lag* atau *bug*.	R12	SIKADU menjadi lambat serta beberapa fitur tidak dapat digunakan.	4	4
Server SIKADU mengalami *down*.	R13	SIKADU tidak dapat diakses sehingga menghambat proses administrasi dan akademik	1	3
Kerusakan *hardware* yang digunakan pada SIKADU.	R14	Penurunan kinerja *hardware* yang mengakibatkan lambatnya respon sistem dan sistem tidak dapat dibuka.	3	2
Kerusakan *software*	R15	Kehilangan data, sistem terganggu sehingga menghambat proses administrasi dan akademik sekolah, dan terjadi kegagalan atau kesalahan dalam melakukan pemrosesan atau penyimpanan data	1	2

	Server SIKADU mengalami o*verload*	R16	Kinerja *server* menjadi lambat, penurunan kecepatan jaringan, dan kerusakan perangkat keras	2	2
	Virus menyerang SIKADU.	R17	Kerusakan data, menghambat kinerja sistem, dan penyebaran virus ke perangkat lain.	1	3
	Server SIKADU tidak dapat terhubung ke jaringan internet.	R18	SIKADU hanya dapat diakses di dalam jaringan lokal sekolah.	2	1
	Pengguna kurang memahami sistem dikarenakan tampilan UI/UX pada SIKADU tidak *user friendly*.	R19	Menyulitkan pengguna ketika mencari menu pengelolaan data yang dibutuhkan pada SIKADU.	2	3
	SIKADU tidak dapat menyimpan perubahan data.	R20	Data yang diubah tidak dapat tersimpan dan data yang ditampilkan tidak *valid*.	2	4
Hasil pengelolaan data pada SIKADU.	Hasil input raport tidak dapat dicetak.	R21	Siswa tidak dapat menerima hasil tes atau ujian.	3	2
	Kehilangan atau pencurian data melalui sistem keamanan data pada SIKADU.	R22	Penyalahgunaan data oleh pihak yang tidak bertanggung jawab.	1	4

Evaluasi risiko dilakukan untuk memetakan risiko yang telah ditemukan dan dinilai pada identifikasi risiko dan analisis risiko menggunakan matriks seperti yang disajikan pada Tabel 5. Dengan keterangan matriks evaluasi risiko sebagai berikut: *high* 19-25 (risiko tinggi), *medium* 7-18 (risiko sedang), dan *low* 1-6 (risiko rendah).

Tabel 5. Matriks Evaluasi Risiko SIKADU

Likelihood						
	Certain	11	16	20	23	25
	Likely	7	12	17	21	24
	Possible	4	8	13	18	22
	Unlike	2	5	9	14	19
	Rare	1	3	6	10	15
		Insignificant	*Minor*	*Moderate*	*High*	*Major*
		Impact				

Hasil evaluasi risiko dari sistem informasi sekolah terpadu (SIKADU) disajikan pada Tabel 6 dalam bentuk matriks evaluasi risiko berdasarkan kriteria *likelihood* dan kriteria *impact*. Selanjutnya pemetaan risiko berdasarkan tingkatan risiko disajikan pada Tabel 7.

Tabel 6. Matriks Hasil Evaluasi Risiko SIKADU

Likelihood						
	Certain					
	Likely			R03	R11, R12	
	Possible		R06, R08, R10, R14, R21	R07		
	Unlike	R05, R18	R09, R16	R19	R04, R09, R20	
	Rare		R15	R01, R02, R13, R17	R22	
		Insignificant	*Minor*	*Moderate*	*High*	*Major*
		Impact				

Tabel 7. Pemetaan Risiko Berdasarkan Tingkatan Risiko SIKADU

Kode Risiko	*Likelihood*	*Impact*	Tingkatan Risiko	Analisis
R11	4	4	*High risk (21)*	Risiko koneksi jaringan yang tidak stabil, level risiko *high*, kerugian mencapai > Rp 25 Juta.
R12	4	4	*High risk (21)*	Risiko SIKADU mengalami *lag* atau *bug*, level risiko *high*, kerugian mencapai > Rp 25 Juta.
R03	4	3	*Medium risk (17)*	Risiko u*sername* dan *password* berdasarkan NIS dan tanggal lahir mudah diketahui oleh pihak lain, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R04	2	4	*Medium risk (14)*	Risiko tim IT kurang memahami permasalahan yang terjadi pada SIKADU, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R20	2	4	*Medium risk (14)*	Risiko SIKADU tidak dapat menyimpan perubahan data, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R07	3	3	*Medium risk (13)*	Risiko kesalahan penginputan data pada SIKADU, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R22	1	4	*Medium risk (10)*	Risiko kehilangan atau pencurian data melalui sistem keamanan data pada SIKADU, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R19	2	3	*Medium risk (9)*	Risiko pengguna kurang memahami sistem dikarenakan tampilan UI/UX pada SIKADU tidak *user friendly*, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.

R06	3	2	*Medium risk (8)*	Risiko guru mata pelajaran terlambat menginputkan nilai, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R08	3	2	*Medium risk (8)*	Risiko nilai raport masih dapat diedit meskipun sudah di *print*, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R10	3	2	*Medium risk (8)*	Risiko berkas surat, berkas penunjang data guru dan dokumentasi lomba tidak dapat diunggah ke SIKADU, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R14	3	2	*Medium risk (8)*	Risiko kerusakan *hardware* yang digunakan pada SIKADU, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R21	3	2	*Medium risk (8)*	Risiko hasil input raport tidak dapat dicetak, level risiko *medium*, kerugian mencapai Rp 10 Juta - Rp 25 Juta.
R01	1	3	*Low risk (6)*	Risiko penyalahgunaan hak akses SIKADU, level risiko *low*, kerugian mencapai < Rp 10 Juta.
R02	1	3	*Low risk (6)*	Risiko pembobolan sistem pada saat *login* dikarenakan tidak ada batas maksimal kesalahan *input username* dan *password*, level risiko *low*, kerugian mencapai < Rp 10 Juta.
R13	1	3	*Low risk (6)*	Risiko *Server* SIKADU mengalami *down*, level risiko *low*, kerugian mencapai < Rp 10 Juta.
R17	1	3	*Low risk (6)*	Risiko virus menyerang SIKADU, level risiko *low*, kerugian mencapai < Rp 10 Juta.
R16	2	2	*Low risk (5)*	Risiko *server* SIKADU mengalami o*verload*, level risiko *low*, kerugian mencapai < Rp 10 Juta.
R09	2	2	*Low risk (5)*	Risiko grafik poin pelanggaran dan grafik nilai yang ditampilkan pada SIKADU tidak sesuai dengan data yang diinputkan, level risiko *low*, kerugian mencapai < Rp 10 Juta.
R15	1	2	*Low risk (3)*	Risiko kerusakan *software*, level risiko *low*, kerugian mencapai< Rp 10 Juta.
R05	2	1	*Low risk (2)*	Risiko fitur atau konten pada SIKADU sudah tidak relevan, level risiko *low*, kerugian mencapai < Rp 10 Juta.
R18	2	1	*Low risk (2)*	Risiko *server* SIKADU tidak dapat terhubung ke jaringan internet, level risiko *low*, kerugian mencapai < Rp 10 Juta.

Perlakuan risiko

Perlakuan risiko memiliki tujuan memberikan saran dan rekomendasi yang dapat digunakan Tim IT SMKN 2 Salatiga sebagai acuan dalam mengatasi risiko. Perlakuan risiko disajikan pada Tabel 8 yang diurutkan berdasarkan tingkatan risiko dari tingkatan tinggi ke tingkatan rendah.

Tabel 8. Perlakuan risiko

Kode Risiko	Tingkatan Risiko	Perlakuan risiko
R11	*High risk (21)*	Melakukan *maintenance* jaringan secara berkala dan menghubungi pihak penyedia layanan jaringan untuk pengecekan dan perbaikan koneksi internet.
R12	*High risk (21)*	Melakukan *update software* dan perbaikan pada bagian yang mengalami *lag* atau *bug*.
R03	*Medium risk (17)*	Memperkuat keamanan dengan autentifikasi yang kuat, mengganti *password*.
R04	*Medium risk (14)*	Melakukan pelatihan secara mandiri dan mencari *problem solving* melalui internet atau sumber sumber terpercaya lainnya.
R20	*Medium risk (14)*	Memeriksa koneksi internet, memperbaharui perangkat lunak ke versi yang lebih baru, pemeliharaan rutin agar kinerja sistem optimal.
R07	*Medium risk (13)*	Memvalidasi data yang akan diinputkan dan melakukan *double check* data yang sudah diinputkan.
R22	*Medium risk (10)*	Meningkatkan sistem keamanan data pada SIKADU serta melakukan *backup* secara rutin.
R19	*Medium risk (9)*	Memperbarui desain UI/UX agar lebih *user friendly*, dokumentasi yang jelas agar memudahkan pengguna mengakses SIKADU.
R06	*Medium risk (8)*	Membuat jadwal batas waktu maksimal penginputan nilai, membuat sistem pengingat.
R08	*Medium risk (8)*	Memblokir pengeditan setelah pencetakan, membuat histori perubahan.
R10	*Medium risk (8)*	Memeriksa batas ukuran *file*, memperbarui perangkat lunak, menggunakan format yang sesuai, memastikan koneksi internet yang stabil.
R14	*Medium risk (8)*	Melakukan *maintenance* pada *hardware* dan mengganti *hardware* yang telah rusak.
R21	*Medium risk (8)*	Memastikan koneksi jaringan stabil, memastikan nilai raport sudah diisi sesuai dengan capaian masing-masing siswa.
R01	*Low risk (6)*	Memastikan setiap pengguna memiliki hak akses dan memberikan kebijakan yang sesuai serta menerapkan teknik penyaringan akses, seperti *firewall* atau kontrol akses berbasis peran.
R02	*Low risk (6)*	Tim IT menambahkan program yang digunakan untuk membatasi maksimal kesalahan penginputan *username* dan *password* saat login SIKADU.
R13	*Low risk (6)*	Melakukan *maintenance* server secara rutin dan berkala.
R17	*Low risk (6)*	Memperbaharui perangkat lunak secara berkala, menggunakan sistem perangkat lunak yang memiliki keamanan kuat dan program antivirus serta melakukan *backup* secara berkala.
R16	*Low risk (5)*	Melakukan pemantauan sistem untuk melihat kinerja dan penggunaan sumber daya, mengoptimalkan aplikasi atau proses yang mengonsumsi banyak sumber daya, melakukan *backup* dan pemulihan jika terjadi kegagalan sistem.
R09	*Low risk (5)*	Melakukan pengecekan fungsi SIKADU dan melakukan *update* sistem.
R15	*Low risk (3)*	Melakukan *update software*, melakukan *backup* data.
R05	*Low risk (2)*	Menghapus fitur atau konten yang sudah tidak sesuai, membuat fitur atau konten baru yang sesuai dengan kebutuhan sekolah.
R18	*Low risk (2)*	Melakukan pemeriksaan dan perbaikan konfigurasi jaringan, memastikan server terhubung dengan *router* atau *switch*, menghubungi penyedia layanan internet untuk memastikan tidak ada permasalahan dengan ISP.

Pemantauan dan peninjauan

Pemantauan dan peninjauan dilakukan bersama Tim IT SMKN 2 Salatiga untuk mengkomunikasikan hasil implementasi dari manajemen risiko dan memastikan pengendalian risiko berjalan dengan baik.

4. KESIMPULAN

Riset ini menghasilkan dokumen tentang analisis manajemen risiko pada sistem informasi sekolah terpadu (SIKADU) SMKN 2 Salatiga menggunakan standar ISO 31000:2018. Riset menemukan 22 kemungkinan risiko yang dapat menghambat bahkan menghentikan kinerja SIKADU sehingga berdampak pada terganggunya aktivitas pelayanan administrasi akademik sekolah. 22 kemungkinan risiko, terbagi dalam tiga level risiko yang berbeda. Pertama, terdapat dua kemungkinan risiko pada level *high*, yaitu koneksi jaringan tidak stabil (R11) dan sistem mengalami *lag* atau *bug* (R12). Kedua, terdapat sebelas kemungkinan risiko pada level *medium*, yaitu *username* dan *password* mudah diketahui oleh pihak lain (R03), tim IT kurang memahami permasalahan yang terjadi pada sistem (R04), sistem tidak dapat menyimpan perubahan data (R20), kesalahan penginputan data pada sistem (R07), kehilangan atau pencurian data melalui sistem keamanan data (R22), pengguna kurang memahami sistem dikarenakan tampilan UI/UX tidak *user friendly* (R19), guru mata pelajaran terlambat menginputkan nilai (R06), nilai raport masih dapat diedit meskipun sudah di *print* (R08), berkas dan dokumentasi tidak dapat diunggah ke sistem (R10), kerusakan *hardware* yang digunakan pada sistem (R14) dan hasil input raport tidak dapat dicetak (R21). Ketiga, terdapat sembilan risiko dengan level *low* yaitu, penyalahgunaan hak akses sistem (R01), pembobolan sistem pada saat *login* dikarenakan tidak ada batas maksimal kesalahan *input username* dan *password* (R02), *server* sistem mengalami *down* (R13), virus menyerang sistem (R17), *server* sistem mengalami *overload* (R16), grafik yang ditampilkan pada sistem tidak sesuai dengan data yang diinputkan (R09), kerusakan *software* (R15), fitur atau konten pada sistem sudah tidak relevan (R05) dan *server* sistem tidak dapat terhubung ke jaringan internet (R18).

SMKN 2 Salatiga sudah lama menggunakan SIKADU untuk pelayanan administrasi dan akademik, namun kinerja sistem belum berjalan secara optimal. Oleh karena itu, riset ini dilakukan untuk melakukan pengelolaan risiko pada aplikasi SIKADU, sehingga sekolah dapat memiliki acuan untuk meminimalisir dan mengelola risiko. Dengan meminimalisir dan mengelola risiko diharapkan kinerja sistem dapat berjalan secara efektif dan efisien menunjang kegiatan administrasi dan akademik di sekolah.

DAFTAR PUSTAKA

[1] M. A. Purba and A. D. Yando, “Pemanfaatan Teknologi Informasi dalam Pendidikan dan Pembelajaran di Era Revolusi Industri 4.0,” *Pros. Semin. Nas. Ilmu Sos. dan Teknol.*, vol. 2, no. 3, pp. 96–101, 2020.

[2] U. Kasma, “Peranan Teknologi Informasi Dalam Mendukung Proses Belajar Siswa,” *Sindimas*, pp. 144–148, 2019.

[3] J. Wahyudi, K. Khairil, I. Y. Beti, Y. Yupianti, and ..., “Peran Teknologi Informasi Pada Masa Pandemi Terhadap Kegiatan Belajar Di Sekolah,” *J. Dehasen Untuk …*, vol. 1, no. 2, pp. 55–62, 2022, [Online]. Available:

https://jurnal.unived.ac.id/index.php/dehasenuntuknegeri/article/view/2512

[4] W. F. Worotikan and E. Maria, "Penerapan ISO 31000 : 2018 untuk Manajemen Risiko E-Ticketing Taman Rekreasi XYZ," *KLIK Kaji. Ilm. Inform. dan Komput.*, vol. 3, no. 5, pp. 449–456, 2023.

[5] F. Setiawan, C. Ardita, A. Syarofah, and M. Zaki, "Manajemen Resiko Di MI Muhammadiyah Kenteng," *LEADERIA J. Manaj. Pendidik. Islam*, vol. 2, no. 2, pp. 62–70, 2021, doi: 10.35719/leaderia.v2i2.69.

[6] S. Suyitno, "Implementasi Manajemen Resiko dalam Peningkatan Efektivitas Pembelajaran di Sekolah Menengah Kejuruan," *Edukatif J. Ilmu Pendidik.*, vol. 4, no. 1, pp. 141–153, 2022, doi: 10.31004/edukatif.v4i1.1768.

[7] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 : 2018 (Studi Kasus: CV. XY)," *Sebatik*, vol. 23, no. 1, pp. 277–284, 2019, doi: 10.46984/sebatik.v23i1.572.

[8] Maximus Ali Perajaka and Yohanes Ngamal, "Pentingnya Manajemen Risiko dalam dunia Pendidikan (Sekolah) Selama dan Pasca Covid-19," *J. Manaj. Risiko*, vol. 2, no. I, pp. 35–50, 2021, doi: 10.33541/mr.v2ii.3436.

[9] 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.

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

[11] V. P. P. Wijaya, "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.

[12] S. S. Syahrial Sidik and W. Wahyuari, "Manajemen Risiko Sistem Informasi Ujian Secara Daring Di Sekolah Tinggi Manajemen Asuransi Trisakti," *J. Green Growth dan Manaj. Lingkung.*, vol. 12, no. 1, pp. 84–97, 2022, doi: 10.21009/10.21009/jgg.v12i1.06.

[13] R. Fahlepi, M. Fronita, E. Saputra, M. . Hamzah, A. Marsal, and S. Daulay, "Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000," *J. Sains Komput. Inform.*, vol. 7, no. 2, pp. 1–14, 2023.

[14] Y. Erlika, M. I. Herdiansyah, and A. H. Mirza, "Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000," *J. Ilm. Inform. Glob.*, vol. 11, no. 1, pp. 55–62, 2020, doi: 10.36982/jiig.v11i1.1073.

[15] M. I. Fachrezi, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000:2018 Diskominfo Kota Salatiga," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 2, pp. 764–773, 2021, doi: 10.35957/jatisi.v8i2.789.

[16] D. P. Natalie and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi dengan ISO 31000:2018 pada PT Bayu Buana Tbk," *JURIKOM (Jurnal Ris.*

Komputer), vol. 9, no. 5, pp. 1290–1301, 2022, doi: 10.30865/jurikom.v9i5.4797.

[17] R. P. Adi, "Analisis Paket Data Pada Jalur Komunikasi SSL dengan Menggunakan Tools Wireshark untuk Keamanan Jalur Komunikasi (Studi Kasus Server Sistem Akademik Terpadu SMK Negeri 2 Salatiga)".

[18] C. P. Setyanti and A. F. Wijaya, "Analisis Pengaruh Perencanaan Strategis SI/TI Dalam Meningkatkan Upaya Keunggulan Bersaing," *J. Softw. Eng. Ampera*, vol. 1, no. 2, pp. 60–70, 2020, doi: 10.51519/journalsea.v1i2.39.

[19] P. I. D. Candra Wulan, D. P. Perdana, A. A. Kurniawan, and R. Fauzi, "Sosialisasi Cyber Security Awareness untuk meningkatkan literasi digital di SMK N 2 Salatiga," *KACANEGARA J. Pengabdi. pada Masy.*, vol. 5, no. 2, pp. 213–218, 2022, doi: 10.28989/kacanegara.v5i2.1204.

[20] A. F. Nasution, *Metode Penelitian Kualitatif*. Bandung: CV. Harfa Creative, 2023.

[21] 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.

[22] C. R. Vorst, D. S. Priyasrono, and A. Budiman, *Manajemen Risiko Berbasis SNI ISO 31000*. Jakarta: Badan Standarisasi Nasional, 2018.