ANALISIS MANAJEMEN RISIKO PADA SISTEM ABSENSI MYSMAMITA MENGGUNAKAN ISO 31000:2018 (STUDI KASUS: SMA MUHAMMADIYAH 1 TAMAN SIDOARJO)

Disusun oleh:

Wijaya Ganda Prasetyo	(1204220048)
Pavita Pramestri	(1204220053)
Nauli Khalila Serafina	(1204220070)
M. Rizky Qoirul H.	(1204220096)
Ferdynal Christian V.	(1204220119)

PROGRAM STUDI SARJANA SISTEM INFROMASI

DIREKTORAT KAMPUS SURABAYA

UNIVERSITAS TELKOM

SURABAYA

2026

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi telah memberikan dampak signifikan terhadap sektor pendidikan, termasuk dalam pengelolaan administrasi dan sistem absensi di sekolah. SMA Muhammadiyah 1 Taman Sidoarjo sebagai lembaga pendidikan yang telah berdiri sejak tahun 1968 terus beradaptasi dengan perkembangan zaman melalui penerapan teknologi informasi dalam berbagai aspek operasionalnya (Rahmatika et al., 2024). Salah satu implementasi teknologi yang diterapkan adalah sistem absensi berbasis teknologi RFID melalui aplikasi MySMAMITA yang tersedia dalam versi *website* dan *mobile*.

Sistem absensi digital MySMAMITA dibangun dengan komponen teknologi informasi yang mencakup hardware (komputer *server*, RFID, *access point*, mini PC), *software* (aplikasi MySMAMITA), data (*database* MySQL untuk siswa, guru, dan absensi), *networking* (Internet, LAN, WiFi), *peopleware* (*programmer* dan *end-user*), serta infrastruktur *server* PCM. Meskipun sistem ini memberikan efisiensi dalam pengelolaan absensi, namun dalam implementasinya terdapat berbagai risiko yang dapat mengganggu operasional sistem dan berdampak pada proses bisnis sekolah.

Berdasarkan observasi yang dilakukan, telah teridentifikasi 25 risiko TI yang pernah terjadi, beberapa diantaranya adalah *server down*, *bug* aplikasi, titip absen antar siswa, *lag* sistem saat diakses bersamaan, wi-fi mati, listrik padam, kehilangan data, pemalsuan dokumen izin, serangan siber, kerusakan modul RFID, kebocoran data pribadi, tidak adanya audit sistem, dan tidak adanya standar keamanan data. Risiko-risiko ini dapat berasal dari berbagai sumber termasuk ancaman siber, kegagalan sistem, dan human error yang semuanya dapat berdampak signifikan terhadap operasional dan reputasi organisasi.

Manajemen risiko teknologi informasi menjadi sangat penting untuk memastikan keberlanjutan operasional dan keamanan informasi. Penelitian ini menggunakan standar ISO 31000:2018 sebagai *framework* untuk mengidentifikasi, menganalisis, mengevaluasi, dan memberikan rekomendasi penanganan risiko pada sistem absensi MySMAMITA (Ayu et al., 2023). Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan efektivitas pengelolaan risiko TI di SMA Muhammadiyah 1 Taman Sidoarjo.

1.2. Rumusan Masalah

Berdasarkan penjelasan pada latar belakang sebelumnya, dapat disimpulkan bahwa permasalahan yang diidentifikasi pada penelitian ini adalah sebagai berikut:

1. Apa saja risiko teknologi informasi yang terdapat pada sistem absensi MySMAMITA di SMA Muhammadiyah 1 Taman Sidoarjo?
2. Bagaimana tingkat prioritas dari setiap risiko teknologi informasi berdasarkan analisis kemungkinan dan dampaknya?
3. Bagaimana strategi penanganan yang tepat untuk memitigasi risiko-risiko teknologi informasi yang teridentifikasi?

1.3. Tujuan Penelitian

Tujuan dari penelitian ini disusun berdasarkan rumusan masalah yang telah dijabarkan sebelumnya, yaitu:

1. Mengidentifikasi risiko-risiko teknologi informasi pada sistem absensi MySMAMITA di SMA Muhammadiyah 1 Taman Sidoarjo menggunakan *framework* ISO 31000:2018.
2. Menganalisis dan mengevaluasi tingkat risiko berdasarkan *likelihood* dan *impact* terhadap operasional sistem.
3. Menyusun rekomendasi strategi mitigasi risiko untuk meminimalkan dampak negatif terhadap sistem absensi MySMAMITA.

1.4. Manfaat Penelitian

1.5.1 Bagi Telkom University Surabaya

1. Memberikan kontribusi akademis dalam bidang manajemen risiko teknologi informasi khususnya pada sistem informasi pendidikan.
2. Menjadi referensi bagi penelitian selanjutnya terkait implementasi ISO 31000:2018 dalam konteks sistem informasi sekolah.

1.5.2 Bagi SMA Muhammadiyah 1 Taman

1. Memperoleh dokumentasi komprehensif mengenai risiko-risiko TI yang ada pada sistem absensi MySMAMITA.
2. Mendapatkan rekomendasi strategi mitigasi risiko yang dapat diimplementasikan untuk meningkatkan keamanan dan keandalan sistem.
3. Menjadi dasar pengambilan keputusan dalam pengembangan kebijakan keamanan informasi sekolah.

1.5.3 Bagi Peneliti

1. Meningkatkan pemahaman dan kompetensi dalam mengaplikasikan *framework* ISO 31000:2018 untuk manajemen risiko TI.
2. Memperoleh pengalaman praktis dalam melakukan analisis risiko pada sistem informasi nyata di lingkungan pendidikan.
3. Mengembangkan kemampuan dalam menyusun rekomendasi strategis untuk pengelolaan risiko teknologi informasi.

BAB II
LANDASAN TEORI

2.1. Dasar Teori

2.1.1. Manajemen Risiko Teknologi Informasi (TI)

Perusahaan sangat bergantung pada teknologi informasi dalam menjalankan proses bisnis untuk mencapai tujuan dari organisasi (Prihandono & Amir, 2024). Sehingga pemanfaatan teknologi informasi memegang peran penting dalam menunjang bisnis. Demi menjaga proses bisnis tetap berjalan dengan optimal, maka hal apapun yang menyangkut dengan teknologi informasi menjadi sangat penting untuk diperhatikan dan dilindungi dengan baik (Fauzi et al., 2023). Semakin pesatnya perkembangan teknologi informasi maka tetap diikuti dengan risiko. Risiko merupakan kemungkinan terjadinya suatu peristiwa yang dapat mempengaruhi pencapaian tujuan organisasi (Vidiarto et al., 2023). Risiko dapat berasal dari berbagai sumber, termasuk ketidakpastian dalam lingkungan eksternal, ketidakpastian dalam pengambilan keputusan, dan ketidakpastian dalam operasional organisasi (Vidiarto et al., 2023). Adanya risiko dapat dicegah dengan adanya manajemen risiko.

Manajemen risiko adalah suatu pendekatan untuk mengidentifikasi, mengevaluasi, dan mengelola risiko terkait dengan aktivitas organisasi (Mardikaningsih et al., 2024). Manajemen risiko mencakup semua aktivitas yang terkait dengan organisasi dan melibatkan faktor perilaku manusia dan budaya serta interaksi dengan para stakeholder. Proses identifikasi risiko ini dilakukan untuk mengenali dan mendokumentasikan risiko-risiko potensial yang dapat mempengaruhi teknologi informasi dan proses bisnis organisasi. Dalam konteks teknologi informasi, manajemen risiko TI mencakup berbagai aspek seperti tata kelola TI, *framework* tata kelola, dan konsep-konsep manajemen risiko yang diterapkan untuk memastikan keberlanjutan operasional dan keamanan informasi. Risiko TI dapat berasal dari berbagai sumber termasuk ancaman siber, kegagalan sistem, dan *human error* yang semuanya dapat berdampak signifikan terhadap operasional dan reputasi organisasi. Setelah proses identifikasi dilakukan, tahapan

selanjutnya yang tak kalah penting adalah evaluasi risiko, karena penting untuk menilai kemungkinan terjadinya dan besarnya dampak yang ditimbulkan (Mardikaningsih et al., 2024).

Evaluasi risiko ini membantu organisasi memprioritaskan risiko mana yang paling kritis dan memerlukan penanganan segera sebelum masuk ke tahap pengelolaan risiko melalui berbagai strategi seperti mengurangi, mentransfer, menerima, atau menghindari risiko tersebut. Penelitian yang dilakukan oleh (Dinata & Kunang, 2024) menemukan bahwa organisasi yang menyesuaikan manajemen risiko TI dengan konteks operasional dan lingkungan eksternal mereka, lebih berhasil dalam mengelola risiko dan meminimalkan dampak negatifnya. Dengan pesatnya perkembangan teknologi yang terus membawa kerentanan baru, manajemen risiko teknologi informasi perlu bersifat adaptif dan terus disesuaikan dengan skala ancaman yang berkembang agar menjadi bagian yang terintegrasi dari tata kelola organisasi yang baik (Dinata & Kunang, 2024; Mardikaningsih et al., 2024).

2.1.2. SMA Muhammadiyah 1 Taman

SMA Muhammadiyah 1 Taman (SMAMITA) didirikan pada tahun 1968 sebagai mainfestasi nyata dari komitmen Muhammadiyah untuk meningkatkan kualitas hidup Masyarakat melalui pendidikan yang mengedepankan ajaran Islam. Dalam perjalanan yang panjang, SMAMITA terus beradaptasi sehingga menjadi sekolah yang unggul dan responsif terhadap perubahan zaman, tetap menyimpan nilai-nilai keislaman dan karakter kebangsaan. Dengan pengalaman yang telah terakumulasi selama lebih dari selama lebih dari lima puluh tahun, SMAMITA tidak hanya berfungsi sebagai lembaga pendidikan, tetapi juga sebagai tempat bagi generasi muda untuk mengembangkan potensi mereka secara maksimal. Adapun visi dan misi yang dimiliki oleh SMAMITA, yaitu:

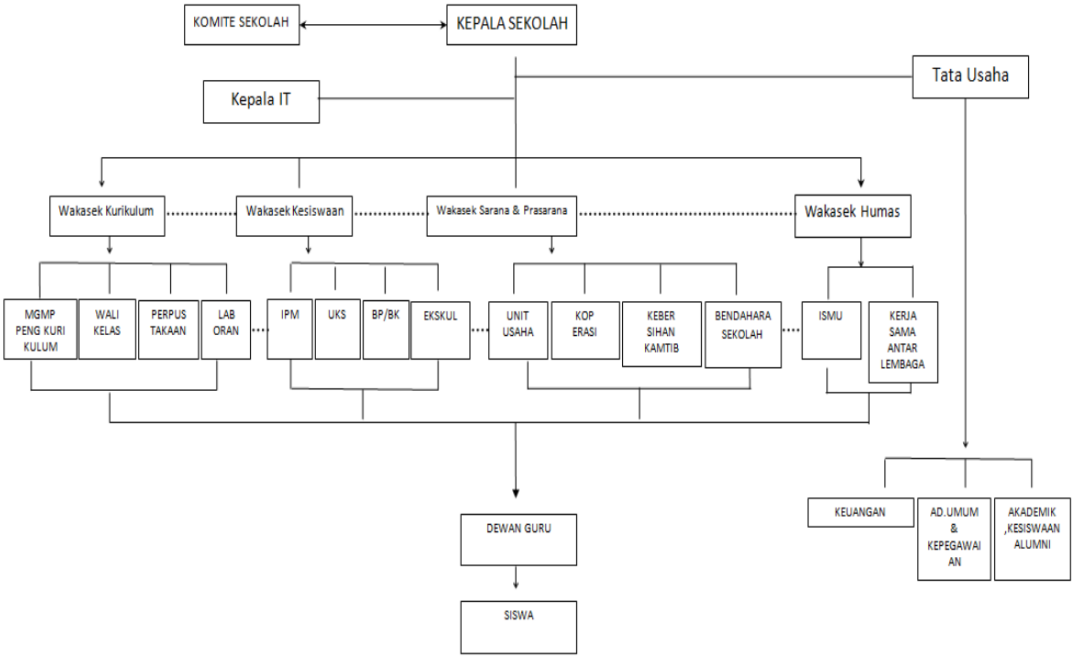
Visi:

Sholeh dalam Perilaku, Unggul dalam Mutu, dan Berdaya Saing Global.

Misi:

a. Menumbuhkan kesadaran seluruh warga sekolah untuk melaksanakan perintah Allah dan menjauhi laranganNya.
b. Mewujudkan generasi Islam yang santun dalam berperilaku dan gemar beribadah.
c. Mengelola dan mengembangkan pendidikan yang berakhlaqul karimah.
d. Mengembangkan potensi akademik dengan menyediakan fasilitas belajar-mengajar dan teknologi informasi.
e. Mengoptimalkan pelayanan akademik dan administrative.
f. Mengoptimalkan proses pembelajaran dan bimbingan intensif kepada peserta didik.
g. Membina kemandirian dalam melaksanakan segala kegiatan.
h. Membangun kerjasama dengan lembaga luar negeri.
i. Meningkatkan kemampuan bahasa asing.
j. Meningkatkan kunjungan dan pertukaran peserta didik serta guru dengan sekolah luar negeri.

Berdasarkan visi "Membentuk siswa yang berperilaku baik, berkualitas tinggi, dan mampu bersaing di tingkat global", SMAMITA menggabungkan nilai-nilai *Religious, Smart, Positive,* dan *Creative* (*RESPECT*) sebagai inti dari nilai-nilai sekolah. Melalui semangat *Respect School,* SMAMITA menciptakan budaya belajar yang aktif, kolaboratif, dan inovatif didukung oleh tenaga pendidik yang professional serta lingkungan yang mendukung. Nilai *RESPECT* menjadi dasar dalam pengembangan karakter siswa agar mereka tumbuh menjadi individu yang beriman, berakhlak baik, berpengetahuan luas, dan siap memberikan kontribusi yang positif bagi masyarakat dan dunia (SMAMITA, n.d.).



Gambar II.1 Struktur organisasi SMA Muhammadiyah 1 Taman

Dalam mencapai misi yang telah ditentukan, SMA Muhammadiyah 1 Taman membagi tugas dan tanggung jawab berdasarkan dengan kapabilitas setiap karyawannya. Oleh sebab itu, untuk memperbaiki struktur organisasi, SMA Muhammadiyah 1 Taman melakukan perubahan pada organisai secara bertahap. Langkah ini diambil dengan harapan dapat menciptakan kegiatan organisasi yang luwes dan responsif, sehingga mampu menyesuaikan diri dengan berbagai situasi dan kondisi yang terus berubah. Gambar II.1 diatas adalah gambar yang menunjukkan struktur organisasi SMA Muhammadiyah 1 Taman.

2.1.3. Aset Teknologi Informasi

Tabel II.1 Aset teknologi informasi

Komponen	Penjelasan	Aset	Merk	Tahun	Jumlah	Tujuan	Risiko	Sumber Risiko	Dampak
Hardware	Perangkat keras yang digunakan untuk menjalankan sistem informasi sekolah	Komputer *Server*	HP	2018	2	*Hosting* aplikasi My SMAMITA dan penyimpanan *database*	*Overheating* dan kehilangan data	**Internal** kegagalan teknis, usia perangkat	Operasional
		Komputer (PC)	Dell	2018	2	Akses sistem My SMAMITA oleh *admin* dan staf TU	Kerusakan *hardware*	**Internal** *human error*, kurang *maintenance*	Operasional

Komponen	Penjelasan	Aset	Merk	Tahun	Jumlah	Tujuan	Risiko	Sumber Risiko	Dampak
		Mini PC	Dell	2020	3	*Monitoring* sistem dan *backup server*	Keterbatasan spesifikasi	**Internal** spesifikasi terbatas	Operasional
		RFID	-	2020	11	Sistem absensi siswa dan guru terintegrasi My SMAMITA	Modul rusak	**Internal & Eksternal** *human error*, faktor lingkungan	Operasional
		Access Point	TP-Link	2021	32	Menyediakan akses internet untuk koneksi My SMAMITA	Gangguan koneksi	**Internal & Eksternal** *bandwidth tidak stabil*	Operasional
Software	Aplikasi dan sistem operasi pendukung	My SMAMITA	-	2020	1	Sistem informasi akademik untuk SMA Muhammadiyah 1 Taman	*Bug* sistem, keamanan, dan *lag*	**Internal** Kurangnya *maintenance,* dan terlalu banyak yang mengakses	Operasional /Keamanan
Data	*Database* dan informasi digital	*Database* Siswa	MySQL	-	-	Menyimpan data pribadi dan akademik siswa	Kebocoran data	**Internal & Eksternal** *human error*, serangan siber	Keamanan/ Legal
		Database Guru			-	Menyimpan data guru dan staf	Kebocoran data	**Internal** *human error*, serangan siber	Keamanan
		Database Absensi			-	Mencatat kehadiran siswa dan guru secara *realtime*	Data tidak terekam, data tidak konsisten	**Internal** kegagalan sistem RFID, koneksi	Operasional
Networking		Internet	Moratel	2019	-	Koneksi utama untuk akses My SMAMITA dan internet sekolah	Putus koneksi, kecepatan lambat	**Eksternal** *provider*, cuaca, gangguan jaringan	
		LAN	Digilink	2019	-	Menghubungkan semua perangkat dalam jaringan internal sekolah	Kabel putus dan *switch* rusak	**Eksternal** *maintenance* kurang	Operasional
		Wi-Fi	Moratel	2019	-	Akses *wireless* untuk My SMAMITA	Wi-Fi mendadak mati	**Eksternal** *provider* cuaca, gangguan jaringan	Operasional
Peopleware		*Programmer*	-	2017	3	*Maintenance* dan *development* My SMAMITA	*Skill* staf kurang memadai	**Internal** SDM kurang *training*	Operasional
		End-User	-	2024	700	Pengguna My SMAMITA	Salah *input* data, kurang sosialisasi	**Internal** *human error*, *awareness* kurang	Operasional

Komponen	Penjelasan	Aset	Merk	Tahun	Jumlah	Tujuan	Risiko	Sumber Risiko	Dampak
Process	Proses dan prosedur TI	*Firewall*	Windows Defender Firewall	2019	-	Keamanan jaringan dari akses tidak *authorized*	*Firewall* tidak ter-*update*	**Internal** *maintenance* kurang	Keamanan
Infrastruktur	Fasilitas pendukung	*Server* PCM (Pimpinan Cabang Muhammadiyah)	Dell	2018	3	*Backup* data dan koordinasi sistem dengan PCM	Ketergantungan pada *server* pusat	**Eksternal** kebijakan PCM, *maintenance* PCM	Operasional

2.2. Penelitian Terdahulu

Pada bagian ini menjelaskan sejumlah penelitian sebelumnya yang relevan dengan penelitian saat ini. Penelitian-penelitian ini penting karena mereka memberikan kerangka teoritis, sumber ide, dan suatu cara untuk mengetahui seberapa banyak penelitian yang telah dilakukan pada suatu topik tertentu. Meskipun objek serta tujuan dari penelitian yang digunakan berbeda, tabel yang disajikan di bawah ini menjelaskan penelitian yang telah ada sebelumnya dan menunjukkan hubungan dengan penelitian sebelumnya.

Tabel II.2 Penelitian terdahulu

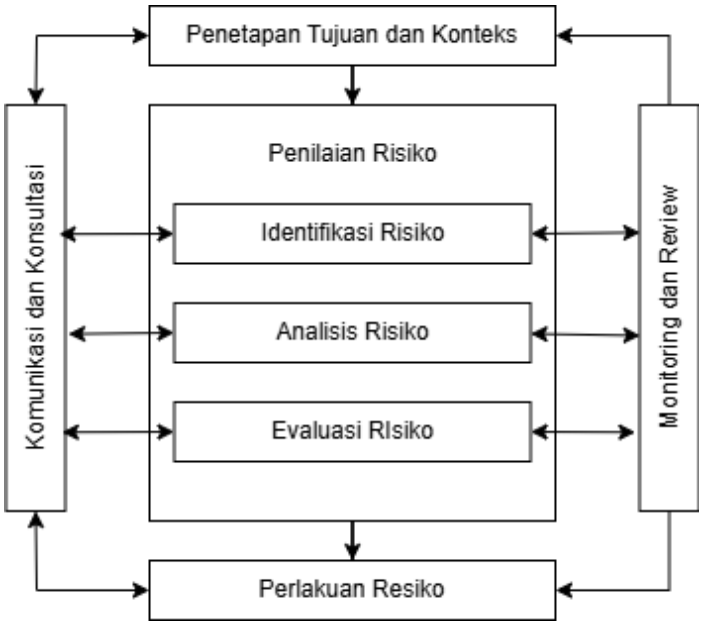
Jurnal Terdahulu	Fokus Penelitian	Standar/Metode	Objek Penelitian	Keterhubungan dengan Penelitian
Analisis Manajemen Risiko pada Aplikasi Sistem Informasi Manajemen Sekolah menggunakan ISO 31000:2018 (Sulistiawati & Hartomo, 2024)	Aplikasi sistem informasi manajemen sekolah (SIM STENDZA)	ISO 31000:2018	SMKN 2 Salatiga	Sangat relevan → lingkup sekolah
Information Technology Risk Management in Educational Institutions Using ISO 31000 Frameworks (Putri & Wijaya, 2023)	Manajemen risiko layanan IT (SIAHDU, SIKADU, SISMINDO)	ISO 31000	Institusi pendidikan di Indonesia	Sangat relevan → sektor pendidikan
Risk Management Analysis of SMK Telkom Makassar's Integrated Academic Information System in Compliance	Sistem Informasi Akademik Terpadu (iGracias)	ISO 31000:2018	SMK Telkom Makassar	Sangat relevan → lingkup sekolah dan metodologi ISO 31000: 2018

Jurnal Terdahulu	Fokus Penelitian	Standar/Metode	Objek Penelitian	Keterhubungan dengan Penelitian
with ISO 31000 Standards (Sahibu et al., 2024)				
Information Technology Risk Management on Semarang Regency BPS Application Using ISO 31000:2018 (Gita & Tanaem, 2022)	Aplikasi *Integrated Collection System* (ICS)	ISO 31000:2018	BPS	Relevan → metodologi ISO 31000:2018
Manajemen Risiko Sistem Informasi menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto (Setiawan et al., 2021)	Sistem Informasi Tripio Purwokerto (*Website* penjualan dan *Point of Sales*)	ISO 31000:2018 dan ISO/EIC 27001:2013	Tripio Purwokerto	Relevan → metodologi ISO 31000:2018

Berdasarkan hasil tinjauan dari penelitian terdahulu, tampak bahwa sebagian besar membahas manajemen risiko sistem informasi dengan memanfaatkan standar ISO 31000, khususnya pada versi ISO 31000:2018. Sebagian besar penelitian dilakukan di sektor pendidikan, seperti sekolah menengah kejuruan dan institusi pendidikan, dengan berfokus pada sistem informasi manajemen dan sistem informasi akademik. Di samping itu, ada juga penelitian yang menerapkan standar ISO 31000:2018 pada sektor pemerintahan dan perusahaan, yang menunjukkan bahwa standar ini memiliki sifat yang adaptif dan dapat digunakan di berbagai organisasi. Meskipun begitu, belum ada penelitian terdahulu yang secara spesifik menganalisa manajemen risiko pada sistem absensi. Berdasarkan hal tersebut, penelitian ini dilakukan untuk menganalisis manajemen risiko pada sistem absensi dengan memanfaatkan standar ISO 31000:2018 karena standar ini dapat diterapkan diberagam jenis sistem dan sektor, sehingga diharapkan dapat memberikan hasil analisis risiko secara menyeluruh dan sesuai dengan kebutuhan sistem yang sedang diteliti.

BAB III
METODOLOGI PENELITIAN

3.1. Alur Penelitian



Gambar III.1 Alur penelitian

3.1.1. Komunikasi dan Konsultasi

Tujuan dari fase komunikasi dan konsultasi adalah untuk memfasilitasi pemangku kepentingan dalam mengenali risiko, membuat keputusan, dan menangani risiko yang ada. Dengan demikian, fase komunikasi dan konsultasi memiliki peranan yang vital dan diharapkan dapat memberikan dukungan pada manajemen risiko agar berjalan dengan benar.

3.1.2. Penetapan Tujuan dan Konteks

Pada fase ini, merupakan fase penentuan sasaran, cakupan, dan bagian organisasi yang akan terlibar dalam manajemen risiko. Ada empat aspek yang harus ditentukan pada fase ini yaitu konteks internal, konteks eksternal, konteks manajemen risiko, dan konten kriteria risiko (Fachrezi et al., 2021).

3.1.3. Penilaian Risiko

Pada fase ini bertujuan untuk mengenali potensi risikio yang terkait dengan aset teknologi informasi dengan mamhami peluang munculnya suatu risiko dan efeknya pada aset teknologi informasi di SMA Muhammadiyah 1 Taman Sidoarjo.

3.1.4. Identifikasi Risiko

Tujuan dari pengenalan risiko adalah untuk menemukan, mengenali, serta menjelaskan risiko berdasarkan informasi yang diperoleh. Data yang relevan dan tepat sangat penting dalam proses pengenalan risiko (Fachrezi et al., 2021).

3.1.5. Analisis Risiko

Tahap ini adalah fase yang menetapkan status risiko dalam kategori kemungkinan frekuensi. Tujuan dari evaluasi risiko adalah untuk mengenali karakteristik dan sifat dari risiko tersebut. Penilaian risiko dapat dijalankan dengan berbagai tingkat kedalaman dan kerumitan, bergantung pada tujuan evaluasi serta informasi yang tersedia (Fachrezi et al., 2021).

3.1.6. Evaluasi Risiko

Pada fase ini, dilakukan evaluasi hasil analisis risiko dengan standar risiko yang telah ditentukan sebelumnya. Sasaran dari fase ini adalah untuk menentukan seberapa besar atau kecil prioritas risiko yang ada serta tingkat risiko mana yang perlu mendapatkan perhatian lebih lanjut (Fachrezi et al., 2021).

3.1.7. Perlakuan Risiko

Tahap ini adalah langkah-langkah untuk menyaring dan mengimplementasikan solusi demi mengurangi kemungkinan terjadinya risiko. Sasaran dari penanganan risiko adalah untuk menentukan serta melaksanakan langkah-langkah dalam mengatasi risiko (Fachrezi et al., 2021).

3.1.8. *Monitoring* dan *Review*

Tahap ini seharusnya menjadi elemen dari strategi pengelolaan risiko. Sasaran dari tahap ini adalah untuk memastikan bahwa pelaksanaan pengelolaan risiko dilakukan sebagaimana mestinya. Hasil dari tahap pemantauan dan evaluasi dipakai sebagai pertimbangan terhadap kemajuan dalam proses pengelolaan risiko (Fachrezi et al., 2021).

3.2. Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan dengan observasi dan wawancara di SMA Muhammadiyah 1 Taman Sidoarjo dengan objek penelitiannya berupa aplikasi absensi guru dan siswa MySMAMITA berbasis website dan mobile. Gambaran menyeluruh kondisi sistem IT yang digunakan, meliputi komponen IT, serta risiko-risiko yang pernah terjadi dalam penerapan sistem absensi tersebut.

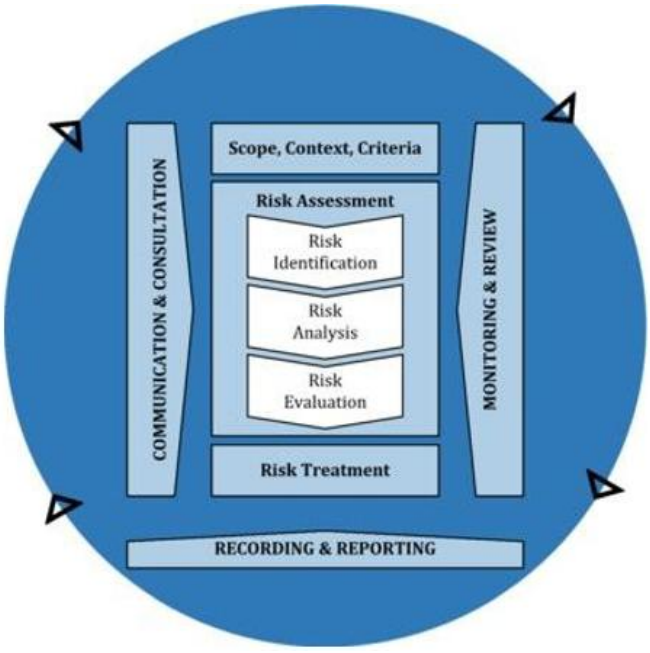
Data yang dikumpulkan mencakup komponen teknologi informasi, yakni hardware seperti komputer server, perangkat RFID, access point, dan PC, dengan software nya berupa aplikasi MySMAMITA, dan data yang dikelola pada sistem menggunakan MySQL berisi database siswa, database guru, dan database absensi. Selain itu, aspek jaringan yang digunakan seperti internet, LAN, dan Wi-Fi juga menjadi bagian dari observasi. Dalam sisi sumber daya manusia, data dari programmer sebagai pengembang sistem dan end-user sebagai pengguna aplikasi. Proses pendukung seperti penggunaan firewall serta infrastruktur server yang berada di Server PCM turut dianalisis untuk memahami alur kerja dan pengamanan sistem secara keseluruhan.

3.3. ISO 31000:2018

ISO 31000:2018 adalah standar internasional dalam manajemen risiko sebagai penyedia prinsip, kerangka kerja serta proses yang dapat diimplementasikan ke dalam berbagai macam organisasi, termasuk dalam institusi pendidikan. Standar dirancang agar dapat menyesuaikan kebutuhan organisasi termasuk dalam pengelolaan risiko IT di sektor pendidikan. Untuk mengelola risiko IT dalam sistem absensi MySMAMITA di SMA Muhammadiyah 1 Taman Sidoarjo

ini digunakan ISO 31000:2018 sebagai pedoman agar berjalan sistematis dan berkelanjutan.

Implementasi dari manajemen risiko pada penelitian ini berdasar pada proses ISO 31000:2018 yang mencakup *Communication & Consultation*, *Scope, Context & Criteria, Risk Assesment, Risk Treatment, Recording & Reporting* serta *Monitoring & Review.* Proses ini bersifat siklus dan berkesinambungan (Setiawan, Sekarini, Waluyo & Afiana , 2021) dengan alurnya dapat dilihat pada Gambar III.2.



Gambar III.2 Proses manajemen risiko

Tahap *Communication & Consultation* ini prosesnya melibatkan pihak yang bersangkutan melalui wawancara dan diskusi bersama pihak sekolah seperti pengelola dan pengguna sistem absensi MySMAMITA. Hal tersebut bertujuan mengulik informasi lebih dalam terkait kondisi sistem yang sudah ada, permasalahan *existing* dan juga potensi risiko yang mungkin muncul (Putri & Wijaya, 2023).

Tahap selanjutnya yaitu S*cope, Context & Criteria* dilakukan guna menetapkan dasar penilaian risiko dan batasan penelitian. Lingkup penelitian berfokus dalam sistem absensi MySMAMITA berbasis *mobile & website.* Terkait konteks terbagi atas 2 sisi yaitu bagi internal kondisi infrastruktur IT, SDM dan operasional sekolah, untuk konteks eksternalnya mencakup faktor lingkungan, vendor dan gangguan eksternal lainnya. Tahapan ini juga menentukan kriteria

risiko untuk mengetahui *likelihood* atau tingkat kemungkinan terjadinya risiko dan *impact* atau tingkat dampak yang ditimbulkan (ISO, 2018).

Tahap *Risk Assesment* atau penilaian risiko terdiri atas 3 proses utama, meliputi identifikasi risiko, analisis risiko, dan evaluasi risiko. Identifikasi dilakukan dengan mencari tahu asset IT dan potensi ancaman uang mungkin mengganggu jalannya sistem absensi. Analisis risiko menilai setiap risiko yang telah diidentifikasi dari tingkat kemungkinan dan dampaknya. Berikutnya, evaluasi risiko didapat dari hasil analisis risiko yang kemudian ditentukan tingkat prioritas risiko nya untuk mengetahui mana risiko yang dapat diterima dan mana yang perlu penanganan lebih lanjut (Setiawan, Sekarini, Waluyo & Afiana , 2021).

Tahap *Risk Treatment* atau perlakuan risiko terhadap risiko tingkat menengah dan tinggi. Perlakuan risiko berguna dalam mengurangi kemungkinan terjadinya atau meminimalisir dampak yang ditimbulkan, disusun dalam bentuk rekomendasi penanganan risiko. Strategi yang digunakan mencakup pengurangan risiko, penghindaran risiko, pemindahan risiko dan penerimaan risiko dengan disesuaikan tingkat risiko masing-masing (Sahibu, Sakti & Iskandar, 2024) (ISO, 2018).

Tahap *Recording & Reporting* atau pencatatan dan pelaporan, mendokumentasikan seluruh proses manajemen risiko dari hasil identifikasi, analisis, evaluasi sampai ke rekomendasi perlakuan risiko. Dokumentasi berikut berguna sebagai bahan evaluasi dan pengambilan keputusan oleh pihak manajemen sekolah, serta sebagai bukti pelaksanaan manajemen risiko (Sahibu, Sakti & Iskandar, 2024).

Tahap terakhir yaitu *Monitoring & Review* berguna dalam memastikan proses manajemen risiko berjalan berkelanjutan serta tetap relevan dengan kondisi sistem dan lingkungan organisasi yang telah berubah. Monitoring dilaksanakan secara berkala guna menilai efektivitas perlakuan risiko yang sudah diimplementasikan, selain itu juga melakukan identifikasi risiko baru yang mungkin muncul (Sahibu, Sakti & Iskandar, 2024).

BAB IV
HASIL DAN PEMBAHASAN

4.1. Identifikasi Risiko

Pada tahapan identifikasi risiko, dilakukannya identifikasi aset untuk mengetahui aset-aset yang penting bagi organisasi yang memiliki potensi memengaruhi operasional sistem.

Tabel IV.1 Aset-aset penting organisasi

Komponen	Aset
Hardware	Komputer *Server*
	Komputer (PC)
	Mini PC
	RFID
	Access Point
Software	My SMAMITA
Data	*Database* Siswa
	Database Guru
	Database Absensi
Networking	Internet
	LAN
	Wi-Fi
Infrastruktur	*Server* PCM (Pimpinan Cabang Muhammadiyah)

Setelah mengidentifikasi aset yang penting bagi organisasi, dilakukan identifikasi risiko. Tahapan ini penting untuk dilakukan agar dapat menemukan, mengetahui, dan menggambarkan risiko yang muncul selama proses wawancara. Wawancara dilakukan dengan beberapa pihak yang bersangkutan dan bertanggung jawab atas bidang keahlian mereka. Berikut adalah tabel IV.2 yang berisikan beberapa risiko-risiko yang didapati saat wawancara:

Tabel IV.2 Identifikasi risiko

No.	Risiko yang Terjadi
1	*Server down*
2	Wi-Fi mendadak mati
3	Listrik padam
4	*Lag*/Lemot saat diakses bersamaan
5	Serangan Siber (*Hacking*)

No.	Risiko yang Terjadi
6	Terjadi *bug* pada alat absensi
7	Dokumen izin dipalsukan
8	Modul RFID rusak
9	Data pribadi bocor
10	Titip absen antar siswa
11	Proses audit sistem belum berjalan rutin
12	Kehilangan data
13	*Overheating*
14	Keterbatasan spesifikasi Mini PC
15	Kerusakan *hardware* PC
16	Gangguan koneksi
17	Bug pada apliksi MySMAMITA
18	Data absensi tidak terekam dan tidak konsisten
19	Kabel LAN putus
20	*Switch* rusak
21	*Skill* staf kurang memadai
22	Kesalahan *input* data dari *end user*
23	Kurangnya sosialisasi pada pengguna
24	*Firewall* tidak ter-*update*
25	Ketergantungan pada *server* pusat

Selanjutnya, dilakukan identifikasi kerentanan untuk mengetahui kelemahan yang terdapat pada sistem, sehingga berpotensi meningkatkan terjadinya risiko.

Tabel IV.3 Kerentanan sistem

No.	Kerentanan
1	Kapasitas *server* kurang memadai
2	Tidak ada jaringan *wifi* cadangan
3	Kurangnya *bandwith* internet
4	Sistem keamanan yang lemah
5	Sensor *error* atau rusak
6	Modul RFID rusak
7	*Chip reader* melemah
8	Standar keamanan data belum diterapkan
9	Tidak ada audit rutin
10	Tidak ada *backup* rutin

No.	Kerentanan
11	Tidak ada standar risiko
12	Terbatasnya spesifikasi MiniPC
13	Usia perangkat
14	Kurangnya *maintenance* rutin pada sistem dan aset
15	Ketergantungan pada satu *server*
16	SDM yang kurang di-*training*
17	*Human error*
18	Kurangnya *awareness* pada pengguna

4.2. Analisis Risiko

Pada tahapan analisis risiko bertujuan untuk memahami risiko yang terjadi secara detail. Pada tahap ini risiko dipetakan berdasarakan dampak dan frekuensi atau tingkat seringnya terjadi risiko. Tahapan ini menjadi acuan strategi untuk pengambilan keputuan mengenai kemungkinan risiko yang terjadi. Untuk memahami bagaimana *Risk Assessment Matrix* bekerja dalam menganalisis risiko, berikut disajikan visualisasi *matrix* yang digunakan dalam penelitian ini:

			Impact →				
			Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood ↑	Almost Certain (>1 in 10)	5	Medium 5	High 10	Extreme 15	Catastrophic 20	Catastrophic 25
	Likely (1 in 20)	4	Low 4	Medium 8	High 12	Extreme 16	Catastrophic 20
	Occasional (1 in 200)	3	Low 3	Medium 6	High 9	High 12	Extreme 15
	Unlikely (1 in 2000)	2	Very Low 2	Low 4	Medium 6	Medium 8	High 10
	Rare (<1 in 10000)	1	Very Low 1	Very Low 2	Low 3	Low 4	Medium 5

Gambar IV.1 *Risk assessment matrix*

Risk assessment matrix pada Gambar IV.1 merupakan *tools* yang digunakan untuk menganalisis dan memetakan tingkat risiko berdasarkan 2 (dua) parameter utama (Embry et al., 2014), yaitu *likelihood* (kemungkinan terjadinya risiko) yang ditampilkan pada sumbu vertikal dan *impact* (dampak yang ditimbulkan) yang ditampilkan pada sumbu horizontal. *Matrix* ini terdiri dari kombinasi 5 tingkat *likelihood* dan 5 tingkat *impact* yang menghasilkan 25 kemungkinan kombinasi risiko. Pada setiap sel *risk matrix* diisi dengan angka yang merupakan hasil

perkalian dari nilai *likelihood* dan *impact* (*Risk Score = Likelihood × Impact*) (Embry et al., 2014). Penggunaan gradasi warna pada *matrix* berfungsi sebagai indikator tingkat keparahan risiko, dimana warna hijau tua menunjukkan risiko dengan tingkat keparahan paling rendah, sedangkan warna merah gelap menunjukkan risiko dengan tingkat keparahan tertinggi yang bersifat kritis. Selain itu, juga perlu dipahami terlebih dahulu terkait parameter-parameter yang menjadi komponen penyusunnya (*likelihood* dan *impact*). Berikut adalah tabel *likelihood*:

Tabel IV.4 Keterangan *likelihood*

Likelihood	**Kategori**	**Keterangan**
1	Sangat Jarang (*Rare*)	Kejadian yang sangat jarang terjadi 1 / *Century* (satu abad)
2	Jarang (*Unlikely*)	Kejadian yang jarang terjadi 1 / *Decade* (10 tahun)
3	Sesekali terjadi (*Occasional*)	Kejadian yang sesekali terjadi 1 / *year* (per tahun)
4	Sering (*Likely*)	Kejadian yang sering terjadi 1 / *month* (per bulan)
5	Sangat Sering (*Almost Certain*)	Kejadian yang sanagat sering terjadi 1 / *week* (minggu)

Tabel IV.4 diatas menjelaskan mengenai skala seberapa sering risiko terjadi mulai dari sangat jarang (*rare*) yang memiliki nilai 1 sampai dengan sangat sering (*almost certain*) yang memiliki nilai 5. Berikut adalah tabel pemetaan dampak (*impact*) dari risiko:

Tabel IV.5 Keterangan dampak

Nilai Dampak	**Keterangan**
1	Risiko memiliki dampak yang tidak signifikan (*Insignificant*)
2	Risiko memiliki dampak yang kecil (*Minor*)
3	Risiko memiliki dampak yang sedang (*Moderate*)
4	Risiko memiliki dampak yang besar (*Major*)
5	Risiko memiliki dampak yang sangat besar (*Castastrophic*)

Tabel IV.5 diatas menjelaskan mengenai skala dampak yang terjadi ketika risiko yang dipetakan terjadi. Dampak risiko dimulai dari dampak risiko yang tidak signifikan (*insignificant*) yang memiliki nilai 1 sampai dengan dampak yang sangat besar (*Catastrophic*). Berikut adalah tabel analisa risiko dengan nilai *likelihood* dan dampak dari masing-masing risiko:

Tabel IV.6 Hasil analisis risiko berdasarkan *likelihood* dan dampak

No.	Risiko yang Terjadi	*Likelihood*	Dampak
1	*Server down*	2	4
2	Wi-Fi mendadak mati	3	4
3	Listrik padam	3	4
4	*Lag*/Lemot saat diakses bersamaan	4	3
5	Serangan Siber (*Hacking*)	3	5
6	Terjadi *bug* pada alat absensi	4	2
7	Dokumen izin dipalsukan	3	1
8	Modul RFID rusak	3	3
9	Data pribadi bocor	2	5
10	Titip absen antar siswa	3	1
11	Proses audit sistem belum berjalan rutin	2	3
12	Kehilangan data	3	4
13	*Overheating*	4	4
14	Keterbatasan spesifikasi Mini PC	2	3
15	Kerusakan *hardware* PC	2	5
16	Gangguan koneksi	4	4
17	Bug pada apliksi MySMAMITA	3	4
18	Data absensi tidak terekam dan tidak konsisten	4	3
19	Kabel LAN putus	2	5
20	*Switch* rusak	2	5
21	*Skill* staf kurang memadai	3	4
22	Kesalahan *input* data dari *end user*	4	3
23	Kurangnya sosialisasi pada pengguna	4	2
24	*Firewall* tidak ter-*update*	3	5
25	Ketergantungan pada *server* pusat	5	5

Dari tabel VI.6 diatas menjelaskan beberapa risiko yaitu:

1) Risiko pertama adalah *server down* dengan penyebab banyak yang mengakses dalam satu waktu dengan nilai *likelihood* sebesar 2 dan dampak 4 yang menyebabkan proses absensi tidak dapat dilaksanakan tepat waktu.
2) Risiko kedua yaitu wifi mendadak mati dengan penyebab dari external atau provider yang menyediakan wifi dengan nilai *likelihood* sebesar 3 dan dampak 4 yang menyebabkan data absensi tidak dapat terkirim.

3) Risiko ketiga yaitu listrik padam dengan penyebab pemadaman masal dengan nilai *likelihood* sebesar 3 dan dampak 4 yang menyebabkan alat berhenti beroperasi.
4) Risiko keempat yaitu *lag*/lemot saat diakses bersamaan dengan penyebab terlalu banyak *user* yang mengakses dalam waktu yang sama dengan nilai *likelihood* sebesar 4 dan dampak 3 yang menyebabkan kesulitan untuk izin dan memasukkan jurnal.
5) Risiko kelima yaitu serangan siber (*hacking*) dengan penyebab lemahnya sistem keamanan dengan nilai *likelihood* sebesar 3 dan dampak 5 yang menyebabkan sistem tidak dapat diakses.
6) Risiko keenam yaitu terjadi *bug* pada alat absensi dengan penyebab sensor rusak, masalah *wiring*, *error software* dengan nilai *likelihood* sebesar 4 dan dampak 2 yang menyebabkan proses absensi berjalan lama dan terjadi redudansi data.
7) Risiko ketujuh yaitu dokumen izin dipalsukan dengan penyebab kurangnya proses verifikasi dengan nilai *likelihood* sebesar 3 dan dampak 1 yang menyebabkan kepercayaan pada sistem menurun.
8) Risiko kedelapan yaitu modul RFID rusak dengan penyebab kerusakan *hardware*, *chip reader* melemah dengan nilai *likelihood* sebesar 3 dan dampak 3 yang menyebabkan absensi otomatis tidak berjalan dengan baik.
9) Risiko kesembilan yaitu data pribadi bocor dengan penyebab standar keamanan data belum diterapkan dengan nilai *likelihood* sebesar 2 dan dampak 5 yang menyebabkan privasi pengguna terancam.
10) Risiko kesepuluh yaitu titip absen antar siswa dengan penyebab kurangnya tanggung jawab siswa, karena terlambat dengan nilai *likelihood* sebesar 3 dan dampak 1 yang menyebabkan data kehadiran tidak akurat.
11) Risiko kesebelas yaitu proses audit sistem belum berjalan rutin dengan penyebab tidak ada *monitoring* berkala dengan nilai *likelihood* sebesar 2 dan dampak 3 yang menyebabkan banyak bug yang tidak ter *tracking.*
12) Risiko keduabelas yaitu kehilangan data dengan penyebab tidak ada *backup* rutin dengan nilai *likelihood* sebesar 3 dan dampak 4 yang menyebabkan data penting hilang permanen.

13) Risiko ketigabelas yaitu overheating dengan penyebab usia perangkat dengan nilai *likelihood* sebesar 4 dan dampak 4 yang menyebabkan perangkat tidak bisa digunakan.
14) Risiko keempatbelas yaitu keterbatasan spesifikasi Mini PC dengan penyebab spesifikasi terbatas dengan nilai *likelihood* sebesar 2 dan dampak 3 yang menyebabkan perangkat tidak dapat memenuhi kebutuhan teknologi terbaru.
15) Risiko kelimabelas yaitu kerusakan *hardware* PC dengan penyebab *human error* dan kurangnya *maintenance* dengan nilai *likelihood* sebesar 2 dan dampak 5 yang menyebabkan perangkat tidak bisa digunakan.
16) Risiko keenambelas yaitu gangguan koneksi dengan penyebab *bandwith* tidak stabil dengan nilai *likelihood* sebesar 4 dan dampak 4 yang menyebabkan proses absensi dan penggunaan sistem terganggu.
17) Risiko ketujuhbelas yaitu bug pada apliksi MySMAMITA dengan penyebab kurangnya maintenance dengan nilai *likelihood* sebesar 3 dan dampak 4 yang menyebabkan sistem susah untuk diakses.
18) Risiko kedelapanbelas yaitu data absensi tidak terekam dan tidak konsisten dengan penyebab kegagalan sistem RFID dan koneksi dengan nilai *likelihood* sebesar 4 dan dampak 3 yang menyebabkan pencatatan absensi terganggu dan munculnya anomali data.
19) Risiko kesembilanbelas yaitu kabel LAN putus dengan penyebab kurangnya *maintenance* dengan nilai *likelihood* sebesar 2 dan dampak 5 yang menyebabkan proses absensi tidak dapat dilaksanakan.
20) Risiko keduapuluh yaitu *switch* rusak dengan penyebab iurangnya *maintenance* dengan nilai *likelihood* sebesar 2 dan dampak 5 yang menyebabkan proses absensi tidak dapat dilaksanakan.
21) Risiko keduapuluhsatu yaitu *skill* staf kurang memadai dengan penyebab SDM yang kurang dilatih dengan nilai *likelihood* sebesar 3 dan dampak 4 yang menyebabkan sistem tidak ter-*maintenance* dengan baik.
22) Risiko keduapuluhdua yaitu kesalahan input data dari *end user* dengan penyebab *Human error* dan kurangnya *awareness* dengan nilai *likelihood* sebesar 4 dan dampak 3 yang menyebabkan munculnya anomali data.

23) Risiko keduapuluhtiga yaitu kurangnya sosialisasi pada pengguna dengan penyebab *Human error* dan kurangnya *awareness* dengan nilai *likelihood* sebesar 4 dan dampak 2 yang menyebabkan pengguna kurang mengerti tentang mekanisme sistem.

24) Risiko keduapuluhempat yaitu firewall tidak terupdate dengan penyebab kurangnya *maintenance* dengan nilai *likelihood* sebesar 3 dan dampak 5 yang menyebabkan potensi terkena serangan siber.

25) Risiko keduapuluhlima yaitu ketergantungan pada server pusat dengan penyebab mengikuti kebijakan PCM dengan nilai *likelihood* sebesar 5 dan dampak 5 yang menyebabkan Jika server pusat down maka sistem tidak dapat digunakan.

4.3. Evaluasi Risiko

Pada tahap ini dilakukan perbandingan hasil analisis risiko dengan kriteria risiko yang telah dilakukan pada *risk assessment*. Tujuan dari tahapan ini adalah untuk mengetahui tinggi rendahnya prioritas risiko. Evaluasi risiko dilakukan dengan menggunakan *risk matrix* yang telah dijelaskan pada subbab 4.2, untuk menentukan apakah risiko diterima, ditolak, atau perlu mitigasi. Tabel IV.7 dibawah ini merupaakan hasil evaluasi risiko untuk aplikasi MySMAMITA.

Tabel IV.7 Evaluasi risiko

No.	Risiko yang Terjadi	*Likelihood*	Dampak	*Risk Score*	*Level*
1	*Server down*	2	4	8	Menengah
2	Wi-Fi mendadak mati	3	4	12	Tinggi
3	Listrik padam	3	4	12	Tinggi
4	*Lag*/Lemot saat diakses bersamaan	4	3	12	Tinggi
5	Serangan Siber (*Hacking*)	3	5	15	Tinggi
6	Terjadi *bug* pada alat absensi	4	2	8	Menengah
7	Dokumen izin dipalsukan	3	1	3	Rendah
8	Modul RFID rusak	3	3	9	Tinggi
9	Data pribadi bocor	2	5	10	Tinggi
10	Titip absen antar siswa	3	1	3	Rendah

No.	Risiko yang Terjadi	*Likelihood*	Dampak	*Risk Score*	*Level*
11	Proses audit sistem belum terjadwal	2	3	6	Menengah
12	Kehilangan data	3	4	12	Tinggi
13	*Overheating*	4	4	16	Tinggi
14	Keterbatasan spesifikasi Mini PC	2	3	6	Menengah
15	Kerusakan *hardware* PC	2	5	10	Tinggi
16	Gangguan koneksi	4	4	16	Tinggi
17	*Bug* pada apliksi MySMAMITA	3	4	12	Tinggi
18	Data absensi tidak terekam dan tidak konsisten	4	3	12	Tinggi
19	Kabel LAN putus	2	5	10	Tinggi
20	*Switch* rusak	2	5	10	Tinggi
21	*Skill* staf kurang memadai	3	4	12	Tinggi
22	Kesalahan input data dari *end user*	4	3	12	Tinggi
23	Kurangnya sosialisasi pada pengguna	4	2	8	Menengah
24	*Firewall* tidak ter-*update*	3	5	15	Tinggi
25	Ketergantungan pada *server* pusat	5	5	25	Kritis

Dari tabel IV.7 evaluasi risiko di atas, dapat diketahui bahwa terdapat 1 risiko dengan tingkat kritis, 17 risiko dengan tingkat tinggi, 5 risiko dengan tingkat menengah, dan 2 risiko dengan tingkat rendah. Pemetaan apakah risiko – risiko tersebut akan diterima, ditolak, atau perlu mitigasi akan dijelaskan sebagai berikut:

a) Risiko *Level* Kritis

Risiko dengan *level* kritis (*catastrophic*) merupakan risiko dengan dampak paling berbahaya yang dapat menyebabkan kegagalan total sistem dan kerugian yang sangat besar. Risiko ini memerlukan **tindakan darurat** dan harus menjadi **prioritas tertinggi** dalam **penanganan**.

1. Ketergantungan pada *Server* Pusat (*Risk Score*: 25)

   Ketergantungan penuh pada *server* pusat tanpa adanya sistem *backup* menyebabkan jika *server* pusat mengalami kegagalan, seluruh sistem

MySMAMITA di semua lokasi akan lumpuh total. Risiko ini memiliki *risk score* tertinggi dengan frekuensi *almost certain* dan dampak *catastrophic*, karena jika risiko ini terjadi maka tidak ada satupun proses absensi, akses data, atau fungsi sistem yang dapat berjalan.

b) Risiko *Level* Tinggi

Risiko dengan *level* tinggi memerlukan **tindakan mitigasi segera** dengan prioritas penanganan dibawah *level* kritis, karena dapat memberikan dampak signifikan bagi operasional MySMAMITA.

1. *Overheating* (*Risk Score*: 16)

Risiko ini memiliki frekuensi *likely* dengan dampak *major*, karena terlalu banyak *user* yang mengakses sistem dan *hardware* PC yang bekerja terlalu keras dapat menyebabkan *overheat*.

2. Gangguan Koneksi (*Risk Score*: 16)

Gangguan pada koneksi internet atau jaringan terjadi dengan frekuensi *likely* dan berdampak *major* pada akses sistem, karena mengganggu operasional sistem secara keseluruhan.

3. Serangan Siber (*Hacking*) (*Risk Score*: 15)

Risiko ini memiliki kemungkinan terjadi *occasional* namun dampak yang *catastrophic* karena lemahnya sistem keamanan, sehingga mengakibatkan serangan siber, perubahan data ilegal, pencurian informasi pribadi, hingga kelumpuhan total pada sistem MySMAMITA. Dampaknya sangat signifikan terhadap keamanan, data, dan privasi seluruh pengguna.

4. *Firewall* Tidak Ter-*Update (Risk Score: 15)*

Firewall yang tidak diperbarui secara berkala terjadi dengan frekuensi *occasional* dan berdampak *catastrophic*, karena membuat sistem rentan terhadap serangan siber.

5. Wi-fi Mendadak Mati (*Risk Score*: 12)

Gangguan eksternal dari *provider* terjadi dengan frekuensi *occasional* dan berdampak *major* pada akses sistem yang mengakibatkan data absensi tidak dapat terkirim tepat waktu sehingga mengganggu operasional sistem secara keseluruhan, terutama bagi pengguna yang mengandalkan koneksi Wi-fi sekolah.

6. Listrik Padam (*Risk Score*: 12)

   Meskipun telah ada genset sebagai cadangan, pemadaman masal tetap memiliki kemungkinan *occasional* dengan dampak *major*, karena alat dapat berhenti beroperasi sementara waktu yang mengganggu proses absensi dan akses sistem.

7. *Lag*/lemot Saat Diakses Bersamaan (*Risk Score*: 12)

   Risiko ini memiliki frekuensi tertinggi (*likely*) dengan dampak *moderate*, karena terlalu banyak *user* yang mengakses sistem pada waktu bersamaan, terutama saat jam-jam puncak seperti jadwal absensi masuk dan pulang sekolah.

8. Kehilangan Data (*Risk Score*: 12)

   Risiko ini terjadi *occasional* dengan dampak major, karena dapat berakibat pada data penting (data absensi, data siswa, dan data akademik) hilang permanen jika terjadi kegagalan sistem atau kesalahan operasional.

9. *Bug* pada Aplikasi MySMAMITA (*Risk Score*: 12)

   Bug pada aplikasi MySMAMITA terjadi dengan frekuensi *occasional* dan berdampak *major*, karena dapat menyebabkan fitur-fitur tertentu tidak berfungsi dengan baik atau bahkan aplikasi mengalami *crash*.

10. Data Absensi Tidak Tercatat secara Konsisten (*Risk Score*: 12)

    Risiko ini terjadi dengan frekuensi *likely* dan berdampak *moderate*, karena inkonsistensi pencatatan data absensi dapat menyebabkan kesulitan dalam rekap data kehadiran.

11. *Skill* Staf yang Kurang Memadai (*Risk Score*: 12)

    Kurangnya *skill* staf IT dalam mengelola sistem terjadi dengan frekuensi *occasional* dan berdampak *major*, karena dapat menyebabkan penanganan masalah yang lambat atau ketidakmampuan untuk melakukan *troubleshooting* saat terjadi gangguan.

12. Kesalahan *Input* Data dari *End User* (*Risk Score*: 12)

    Kurangnya *skill* atau kompetensi staf IT dalam mengelola sistem terjadi dengan frekuensi *occasional* dan berdampak *major*, karena dapat menyebabkan penanganan masalah yang lambat, kesalahan dalam

konfigurasi sistem, atau ketidakmampuan untuk melakukan troubleshooting saat terjadi gangguan.

13. Data Pribadi Bocor (*Risk Score*: 10)

    Meskipun frekuensinya *unlikely* karena standar keamanan data belum diterapkan secara optimal, dampak risiko ini *catastrophic* karena terkait privasi pengguna. Kebocoran dapat mengancam keamanan data pribadi siswa, guru, dan informasi sensitif lainnya.

14. Kerusakan *Hardware* PC (*Risk Score*: 10)

    Risiko ini memiliki frekuensi *unlikely* dengan dampak *catastrophic*, karena kerusakan pada hardware PC dapat menyebabkan sistem tidak dapat beroperasi maksimal.

15. Kabel LAN Putus (*Risk Score*: 10)

    Kerusakan fisik pada kabel LAN terjadi dengan frekuensi *unlikely* namun berdampak *catastrophic*, karena dapat menyebabkan putusnya koneksi antara perangkat dengan jaringan.

16. *Switch* Rusak (*Risk Score*: 10)

    Kerusakan pada *switch* jaringan memiliki frekuensi *unlikely* dengan dampak *catastrophic*, karena dapat menyebabkan seluruh perangkat yang terhubung pada *switch* tersebut kehilangan koneksi jaringan.

17. Modul RFID Rusak (*Risk Score*: 9)

    Kerusakan *hardware* atau *chip reader* melemah diidentifikasi terjadi *occasional* dengan dampak *moderate*, karena mengakibatkan absensi otomatis tidak berjalan dengan baik yang mempengaruhi proses pencatatan kehadiran.

c) Risiko *Level* Menengah

Risiko dengan *level* menengah memerlukan **tindakan mitigasi terencana** dan ***monitoring* berkala**, meskipun tidak sesegera seperti risiko dengan *level* tinggi.

1. *Server Down* (*Risk Score*: 8)

   Overload akses dalam satu waktu dan *hardware* yang kurang memadai menyebabkan *server down* dengan frekuensi *unlikely* namun

berdampak *major*. Proses absensi tidak dapat dilaksanakan tepat waktu dan menghentikan seluruh operasional sistem.

2. Terjadi *Bug* pada Alat Absensi (*Risk Score*: 8)

   Error software menyebabkan *bug* terjadi dengan frekuensi *likely* dengan dampak *minor*, karena proses absensi masih berjalan meskipun memakan waktu lama dan terjadi redudansi data.

3. Kurangnya Sosialisasi pada Pengguna (*Risk Score*: 8)

   Kurangnya edukasi dan sosialisasi kepada pengguna sistem terjadi dengan frekuensi *likely* dan berdampak *minor*, karena dapat menyebabkan pengguna tidak memahami cara penggunaan sistem dengan benar.

4. Proses Audit Sistem Belum Terjadwal (*Risk Score*: 6)

   Risiko ini memiliki frekuensi *unlikely* dengan dampak *moderate.* Meskipun risiko ini tidak berdampak langsung pada operasional harian namun dapat menumpuk menjadi masalah yang lebih besar.

5. Keterbatasan Spesifikasi Mini PC (*Risk Score*: 6)

   Spesifikasi Mini PC yang terbatas diidentifikasi terjadi frekuensi *unlikely* namun berdampak *moderate*, karena berakibat terutama pada saat sistem memerlukan pemrosesan data yang lebih berat atau kompleks.

d) Risiko *Level* Rendah

Risiko dengan *level* rendah dapat **diterima** dengan ***monitoring* rutin** karena dampaknya minimal dan tidak seberapa mengganggu operasional MySMAMITA secara signifikan.

1. Dokumen Izin Dipalsukan (*Risk Score*: 3)

   Proses verifikasi yang kurang *strict* menyebabkan kemungkinan pemalsuan terjadi *occasional* dengan dampak *insignificant* karena kepercayaan pada sistem menurun.

2. Titip Absen Antar Siswa (*Risk Score*: 3)

   Kurangnya tanggung jawab siswa dan lemahnya pengawasan dapat menyebabkan titip absen terjadi *occasional* dengan dampak *insignificant* karena hanya berakibat pada data kehadiran yang tidak akurat.

4.4. Rekomendasi Penanganan Risiko

Berdasarkan hasil evaluasi risiko pada sistem absensi MySMAMITA, rekomendasi penanganan risiko disusun dengan mengacu pada nilai *risk score*, *level* risiko, serta usulan tindakan yang terdapat pada *Risk Assessment Matrix*. Rekomendasi difokuskan pada risiko dengan tingkat kritis dan tinggi, kemudian diikuti risiko menengah dan rendah, dengan tujuan menurunkan kemungkinan kejadian maupun dampak yang ditimbulkan

a) Rekomendasi untuk Risiko Tingkat Kritis

Risiko tingkat kritis **wajib dimitigasi** karena memiliki prioritas penanganan paling tinggi karena dapat menghentikan seluruh operasional sistem absensi.

1. Ketergantungan pada *Server* Pusat

Rekomendasi penanganan risiko ketergantungan pada *server* PCM adalah dengan menyediakan *server* cadangan di lingkungan sekolah yang dapat digunakan ketika *server* pusat mengalami gangguan. Selain itu, pihak sekolah dapat mulai mengoptimalkan penggunaan *server* sekolah sendiri agar layanan MySMAMITA tidak sepenuhnya bergantung pada kebijakan dan kondisi *server* pusat.

b) Rekomendasi untuk Risiko Tingkat Tinggi

Risiko tingkat tinggi perlu **segera dimitigasi** karena berdampak signifikan terhadap kelancaran absensi dan ketersediaan layanan.

1. Wi-Fi Mendadak Mati

   Risiko Wi-Fi mendadak mati dapat ditangani dengan cara sekolah segera menghubungi *provider* Wi-Fi ketika terjadi gangguan untuk mendapatkan penanganan secepatnya. Selain itu, pemasangan *router* atau *access point* yang lebih stabil direkomendasikan untuk meningkatkan kualitas dan kestabilan jaringan yang digunakan sistem absensi.

2. Listrik Padam

   Untuk mengurangi dampak listrik padam, sekolah dapat menggunakan genset sebagai sumber listrik cadangan agar perangkat penting tetap dapat beroperasi. Penambahan kapasitas genset juga

direkomendasikan supaya mampu menopang lebih banyak perangkat yang berkaitan dengan sistem absensi ketika terjadi pemadaman.

3. *Lag*/Lemot Saat Diakses Bersamaan

   Risiko *lag* atau lemot ketika banyak pengguna mengakses sistem dapat dikurangi dengan pengaturan akses secara bergantian pada waktu-waktu sibuk agar beban sistem tidak terlalu tinggi dan peningkatan kapasitas *bandwidth* internet diperlukan untuk mendukung akses pengguna yang lebih besar.

4. Serangan Siber (*Hacking*)

   Penanganan risiko serangan siber dilakukan dengan menambah *firewall* sebagai pengaman jaringan sistem MySMAMITA. Pembaruan keamanan seperti *update firewall* dan proteksi lain dilakukan secara berkala untuk mencegah serangan yang memanfaatkan celah keamanan.

5. Modul RFID Rusak

   Jika modul RFID rusak, sekolah dapat menerapkan absensi manual di kelas sebagai solusi sementara agar proses pencatatan kehadiran tetap berjalan. Di samping itu, perlu dilakukan pengecekan modul RFID secara berkala sebelum digunakan untuk memastikan perangkat dalam kondisi baik.

6. Data Pribadi Bocor

   Penanganan risiko kebocoran data pribadi antara lain dengan memberikan himbauan kepada pengguna agar tidak membagikan *username* dan *password* kepada pihak lain. Selain itu, penerapan standar keamanan data seperti enkripsi, *hashing*, atau mekanisme pengamanan setara direkomendasikan untuk melindungi data sensitif pengguna.

7. Kehilangan Data

   Risiko kehilangan data dapat ditangani dengan menerapkan *backup* otomatis harian atau mingguan terhadap *database* yang digunakan pada sistem absensi. Dengan adanya *backup* rutin, data penting dapat dipulihkan ketika terjadi kegagalan sistem atau insiden yang menyebabkan hilangnya data secara permanen.

8. *Overheating*

   Overheating pada perangkat diatasi dengan memastikan sirkulasi udara di sekitar perangkat berjalan dengan baik agar suhu tetap terjaga. Perangkat yang sudah melewati usia pakai juga direkomendasikan untuk diganti demi mengurangi potensi kerusakan akibat panas berlebih.

9. Kerusakan *Hardware* PC

   Untuk menangani kerusakan *hardware* PC, dilakukan pemeriksaan *hardware* oleh tim IT ketika terjadi gangguan pada perangkat. Selain itu, penjadwalan *maintenance hardware* secara rutin perlu diterapkan agar kondisi perangkat tetap terjaga dan risiko kerusakan dapat diminimalkan.

10. Gangguan Koneksi

    Risiko gangguan koneksi dapat dikurangi dengan melakukan *monitoring* koneksi internet secara berkala untuk mengetahui kualitas dan kestabilan jaringan. Rekomendasi lain adalah meningkatkan kapasitas *bandwidth* internet agar sistem absensi dapat digunakan dengan lebih lancar.

11. *Bug* pada Aplikasi MySMAMITA

    Untuk risiko bug pada aplikasi MySMAMITA, perbaikan dilakukan setelah adanya laporan dari pengguna ketika ditemukan masalah pada sistem. Selain itu, *maintenance* dan pengujian sistem secara rutin perlu dilakukan agar *bug* dapat diminimalkan dan aplikasi tetap berjalan stabil.

12. Data Absensi Tidak Terekam dan Tidak Konsisten

    Penanganan risiko ini dilakukan dengan melakukan pengecekan data absensi secara manual oleh wali kelas sebagai langkah verifikasi tambahan. Selain itu, sinkronisasi antara sistem RFID dan jaringan perlu dijalankan untuk memastikan data absensi tercatat dengan baik dan konsisten.

13. Kabel LAN Putus

    Risiko kabel LAN putus dapat dikurangi dengan melakukan perawatan instalasi jaringan secara rutin, termasuk pengecekan kondisi fisik kabel. Pengamanan jalur kabel juga penting agar kabel tidak mudah terganggu oleh aktivitas pengguna atau faktor lingkungan.

14. *Switch* Rusak

    Untuk *switch* yang rusak, tindakan yang dilakukan adalah mengganti *switch* dengan perangkat baru ketika terjadi kerusakan. Sekolah juga perlu menyiapkan *switch* cadangan dan melakukan *maintenance* perangkat jaringan secara rutin untuk mencegah gangguan mendadak.

15. *Skill* Staf Kurang Memadai

    Risiko *skill* staf yang kurang memadai dapat ditangani dengan menyelenggarakan pelatihan teknis rutin bagi staf yang bertanggung jawab terhadap pengelolaan sistem MySMAMITA. Dengan pelatihan, diharapkan staf mampu melakukan pemeliharaan dan penanganan awal ketika terjadi gangguan sistem.

16. Kesalahan *Input* Data dari *End User*

    Penanganan kesalahan *input* data dilakukan dengan validasi data secara manual oleh pihak yang berwenang untuk memastikan kebenaran informasi yang di-*input*. Selain itu, sistem disarankan menyediakan validasi *input* otomatis dan panduan penggunaan yang jelas untuk membantu pengguna mengurangi kemungkinan kesalahan.

17. *Firewall* Tidak Ter-*Update*

    Risiko *firewall* tidak ter-*update* dapat dikurangi dengan menjadwalkan pembaruan *firewall* dan melakukan *monitoring* keamanan sistem secara rutin. Pengelolaan *update* yang terjadwal membantu memastikan sistem tetap terlindungi dari ancaman siber terbaru.

c) Rekomendasi untuk Risiko Tingkat Menengah

Risiko dengan *level* menengah termasuk kategori risiko yang masih **dapat ditoleransi, tetapi tidak sepenuhnya diterima** tanpa tindakan, sehingga tetap memerlukan perlakuan risiko dan monitoring berkala.

1. Server Down

Risiko *server down* dapat dikurangi dengan meningkatkan kapasitas *server*, misalnya menambah *storage*, RAM, dan CPU agar *server* lebih mampu menangani beban akses. Pemanfaatan server sekolah sendiri sebagai bagian dari peningkatan kapasitas juga dapat membantu mengurangi frekuensi gangguan *server* pada saat jam sibuk.

2. Terjadi *Bug* pada Alat Absensi

   Penanganan *bug* pada alat absensi dilakukan dengan pengecekan sensor, *wiring*, dan komponen perangkat secara berkala untuk memastikan kinerja alat tetap baik. Penyediaan alat absensi cadangan juga direkomendasikan sehingga proses absensi tetap dapat dilaksanakan meskipun alat utama mengalami gangguan.

3. Proses Audit Sistem Belum Terjadwal

   Untuk mengatasi belum adanya jadwal audit sistem, sekolah disarankan menyusun jadwal audit sistem secara bulanan atau triwulanan. Audit ini berfungsi untuk memonitor *bug*, celah keamanan, serta kepatuhan terhadap prosedur pengelolaan sistem sehingga kualitas layanan MySMAMITA dapat terus ditingkatkan.

4. Keterbatasan Spesifikasi Mini PC

   Risiko keterbatasan spesifikasi mini PC dapat dikurangi dengan melakukan *upgrade* spesifikasi perangkat agar mampu memenuhi kebutuhan teknologi terbaru yang digunakan sistem. Rencana *upgrade* sebaiknya disusun berdasarkan beban kerja sistem dan prioritas penggunaan mini PC dapat dikurangi dengan melakukan *upgrade* spesifikasi perangkat agar mampu memenuhi kebutuhan teknologi terbaru yang digunakan sistem. Rencana *upgrade* sebaiknya disusun berdasarkan beban kerja sistem dan prioritas penggunaan mini PC dalam kegiatan operasional sekolah.

5. Kurangnya Sosialisasi pada Pengguna

   Penanganan risiko kurangnya sosialisasi dilakukan dengan mengadakan sosialisasi dan edukasi penggunaan sistem secara berkala, tidak hanya pada awal implementasi. Kegiatan ini melibatkan tim IT sekolah dan wakil kepala sekolah terkait sehingga seluruh pengguna memahami cara penggunaan MySMAMITA dengan benar.

d) Rekomendasi untuk Risiko Tingkat Rendah

Risiko tingkat rendah dapat **diterima dengan** tetap diberikan **pengendalian** administratif dan pemantauan agar tidak berkembang menjadi risiko yang lebih tinggi.

1. Dokumen Izin Dipalsukan

   Penanganan risiko ini dilakukan melalui pengecekan ulang dokumen izin oleh bagian administrasi umum dan kepegawaian. Selain itu, penerapan verifikasi *timestamp* pada proses izin direkomendasikan agar keaslian dan waktu pengajuan izin dapat terpantau dengan lebih baik.

2. Titip Absen Antar Siswa

   Risiko titip absen dapat dikurangi dengan pengecekan berulang oleh guru terhadap kehadiran siswa dan konsistensi data absensi. Penguatan aturan kedisiplinan serta pemberian sanksi yang jelas diharapkan dapat meningkatkan tanggung jawab siswa terhadap kehadiran.

Dengan penerapan rekomendasi penanganan risiko tersebut, sistem absensi MySMAMITA di SMA Muhammadiyah 1 Taman diharapkan memiliki tingkat keandalan dan keamanan yang lebih baik, serta selaras dengan hasil penilaian risiko yang telah disusun dalam *Risk Assessment Matrix*.

BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitian yang telah di lakukan di SMA Muhammadiyah 1 Taman Sidoarjo (SMAMITA) terkait manajemen risiko sistem absensi MySMAMITA menggunakan ISO 31000:2018 berjalan melalui beberapa tahapan, yang pertama yaitu identifikasi risiko, lalu dilakukan analisa risiko, setelahnya risiko-risiko tersebut dievaluasi, dan yang terakhir yaitu perlakuan risiko dengan memberikan rekomendasi penanganan risiko.

Pada tahapan pertama yaitu identifikasi risiko didapati sebanyak 25 risiko pada sistem absensi di SMAMITA. Setelah dilakukan analisa dan evaluasi pada 25 risiko tersebut, terdapat 1 risiko yang masuk ke dalam *level* kritis dimana risiko ini harus diberikan penanganan khusus agar dampak yang diberikan berkurang. Pada *level* tinggi terdapat 17 risiko yang membutuhkan perhatian untuk mengurangi dampak pada proses absensi. Selain itu, pada *level* menengah terdapat 5 risiko dan pada *level* rendah terdapat 2 risiko yang dapat ditolerir. Maka dapat disimpulkan bahwa SMA Muhammadiyah 1 Taman perlu melakukan perlakuan risiko untuk mengurangi terjadinya risiko-risiko yang akan datang dan berdampak pada proses absensi di sekolah.

Hasil dari penelitian ini adalah penilaian dan perlakuan risiko berupa rekomendasi penanganan risiko. Selain itu, penelitian ini juga menghasilkan sebuah dokumentasi berupa saran SOP Manajemen Risiko pada Sistem Absensi serta Standar Risiko yang dapat dijadikan sebagai acuan untuk melakukan manajemen risiko di SMA Muhammadiyah 1 Taman Sidoarjo agar risiko-risiko yang teridentifikasi dapat dikelola dengan baik dan terstruktur.

5.2. Saran

Berdasarkan hasil penelitian yang telah dilakukan, disarankan agar pihak SMA Muhammadiyah 1 Taman Sidoarjo menerapkan manajemen risiko yang lebih sistematis dan terdokumentasi, khususnya pada aktivitas absensi guru dan siswa, guna meminimalkan potensi risiko yang dapat mengganggu proses operasional

sekolah. Selain itu, perlu dilakukan penyusunan dan penerapan Standar Operasional Prosedur (SOP) dan standar manajemen risiko yang lebih terstruktur dan komprehensif. Bagi peneliti selanjutnya, disarankan untuk melakukan penelitian dengan cakupan yang lebih luas serta melibatkan lebih banyak narasumber agar informasi terkait risiko yang pernah terjadi dapat diperoleh secara lebih lengkap dan mendalam. Dengan demikian, hasil penelitian diharapkan dapat memberikan kontribusi yang lebih optimal dalam upaya pencegahan dan pengendalian risiko di lingkungan SMA Muhammadiyah 1 Taman Sidoarjo.

DAFTAR PUSTAKA

Dinata, A., & Kunang, Y. N. (2024). Analisis Manajemen Resiko Teknologi Informasi Perusahaan Kesehatan: Health Company Information Technology Risk Management Analysis. *Indonesian Journal of Innovation Multidisipliner Research*, *2*(1), 45–51.

Embry, M. R., Bachman, A. N., Bell, D. R., Boobis, A. R., Cohen, S. M., Dellarco, M., Dewhurst, I. C., Doerrer, N. G., Hines, R. N., & Moretto, A. (2014). Risk assessment in the 21st century: roadmap and matrix. *Critical Reviews in Toxicology*, *44*(sup3), 6–16.

Fachrezi, M. I., Dwika Cahyono, A., & Tanaem, P. F. (2021). Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga. *Jurusan Sistem Informasi*, *8*(2). http://jurnal.mdp.ac.id

Fauzi, A. A., Kom, S., Kom, M., Harto, B., Dulame, I. M., Pramuditha, P., Sos, S., Sudipa, I. G. I., Kom, S., & Dwipayana, A. D. (2023). *Pemanfaatan Teknologi Informasi di Berbagai Sektor Pada Masa Society 5.0*. PT. Sonpedia Publishing Indonesia.

Gita, S., & Tanaem, P. F. (2022). Information Technology Risk Management on Semarang Regency BPS Application Using ISO31000:2018. *Journal of Information Systems and Informatics*, *4*(2). http://journal-isi.org/index.php/isi

Mardikaningsih, R., Halizah, S. N., Nuraini, R., Darmawan, D., & Hardyansah, R. (2024). Manajemen Risiko Pada Penerapan Manajemen Rantai Pasokan Global: Kajian Terhadap Pendekatan Strategis Untuk Mengidentifikasi, Mengevaluasi, dan Mengelola Risiko. *Yos Soedarso Economic Journal (YEJ)*, *6*(2), 1–15.

Prihandono, G., & Amir, M. T. (2024). Implementasi teknologi informasi dalam meningkatkan efisiensi organisasi dan daya saing perusahaan. *Journal of Economics and Business UBS*, *13*(2), 577–587.

Putri, N. L., & Wijaya, A. F. (2023). Information Technology Risk Management in Educational Institutions Using ISO 31000 Framework. *Journal of Information Systems and Informatics*, *5*(2), 630–649. https://doi.org/10.51519/journalisi.v5i2.468

Sahibu, S., Sakti, A., & Iskandar, A. (2024). Risk Management Analysis of SMK Telkom Makassar's Integrated Academic Information System in Compliance with ISO 31000 Standards. *IIETA : International Information and Engineering Technology Association*, *29*(1), 205–218. https://doi.org/10.18280/isi.290121

Setiawan, I., Sekarini, A. R., Waluyo, R., & Afiana, F. N. (2021). Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *20*(2), 389–396. https://doi.org/10.30812/matrik.v20i2.1093

SMAMITA. (n.d.). *Tentang Kami, SMAMITA*. SMA Muhammadiyah 1 Taman.

Sulistiawati, A., & Hartomo, K. D. (2024). Analisis Manajemen Risiko pada Aplikasi Sistem Informasi Manajemen Sekolah Menggunakan ISO 31000:2018. *Sistemasi: Jurnal Sistem Informasi*, *13*(5), 2540–9719. http://sistemasi.ftik.unisi.ac.id

Vidiarto, A., Azis, R., Mulyanto, A., Meidilah, M., Supryanto, S., & Prasetyono, H. (2023). Pengaruh Budaya Peduli Resiko Dalam Meningkatkan Efektivitas Manajemen Resiko Organisasi. *BULLET: Jurnal Multidisiplin Ilmu*, *2*(4), 982–991.

Ayu, S., Pitaloka, D., Maria, E., Informasi, F. T., Kristen, U., & Wacana, S. (2023). *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*. *12*, 477–489.

Rahmatika, A. N., Apriyadi, M. F., & Kahfi, M. A. (2024). *Jurnal Manajemen dan Teknologi Informasi (JMTI) ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA SISTEM INFORMASI AKADEMIK (SIAK)*

UNIVERSITAS MUHAMMADIYAH SUKABUMI (UMM) MENGGUNAKAN ISO 31000. *14*(1), 48–57.

LAMPIRAN

Lampiran 1. Dokumentasi wawancara

SMAMITA
SMA MUHAMMADIYAH 1 TAMAN

Jl. Raya Ketegan No.35, Ketegan, Kec. Taman, Kabupaten Sidoarjo, Jawa Timur 61257

Nomor SOP	SOP/SMAMITA/TI/ABS/01
TGL. Pembuatan	20 Desember 2025
TGL. Revisi	-
TGL. Efektif	20 Desember 2025
Nama SOP	SOP Manajemen Risiko pada Sistem Absensi SMA Muhammadiyah 1 Taman
Disahkan Oleh	**Kepala Sekolah SMA Muhammadiyah 1 Taman**

Dasar Hukum	**Kualifikasi Umum Pelaksana**
Standar ISO 31000:2018 tentang Manajemen Risiko	1. Operator / Admin Sistem MySMAMITA. 2. Tim IT SMA Muhammadiyah 1 Taman. 3. Guru dan Wali Kelas SMA Muhammadiyah 1 Taman. 4. Memahami penggunaan komputer. 5. Memiliki pemahaman dasar pengelolaan sistem absensi.
Keterkaitan	**Peralatan dan Perlengkapan**
1. SOP Pengelolaan Sistem Absensi 2. SOP Pengelolaan dan Pemeliharaan Sarana dan Prasarana Teknologi Informasi Sekolah 3. SOP Pengelolaan Data Akademik	1. Sistem absensi MySMAMITA 2. PC atau Laptop. 3. Internet dan Jaringan. 4. Perangkat pendukung sistem absensi.
Catatan	**Pencatatan dan Pendataan**
1. Data absensi wajib diinput setiap hari pembelajaran 2. Kesalahan input harus segera dilaporkan kepada Admin Sistem 3. Akses sistem bersifat pribadi dan tidak boleh disalahgunakan	1. Data absensi disimpan dalam bentuk data elektronik pada sistem MySMAMITA 2. Data absensi direkap secara harian, mingguan, dan bulanan 3. Backup data dilakukan secara berkala oleh Admin Sistem

NO	Kegiatan	Aktor			Mutu Baku			Keterangan
		Tim IT SMAMITA	Admin Sistem MySMAMITA	Guru/Walikelas	Kelengkapan	Waktu	Output	
1	Melakukan identifikasi potensi risiko pada sistem absensi MySMAMITA				Data sistem absensi	Secara berkala	Daftar potensi risiko	
2	Membuat laporan terkait gangguan yang terjadi pada sistem absensi				Akses pada sistem absensi	Saat terjadi gangguan pada sistem absensi	Daftar gangguan sistem	Dilaporkan ke Tim IT
3	Menganalisa risiko sesuai dengan tingkat kemungkinan (*likelihood*) dan dampaknya atas setiap potensi risiko yang telah teridentifikasi				Daftar potensi risiko	Setelah identifikasi	Hasil analisis risiko	
4	Mengevaluasi hasil analisa risiko dan menentukan skala prioritas risiko				Hasil analisis risiko	Secara berkala	Skala prioritas risiko	
5	Menindaklanjuti hasil analisa: a) Apabila perlu ditindak lanjuti maka dilakukan penyusunan rencana penanganan risiko b) Apabila tidak perlu ditindak lanjuti, maka akan masuk ke batas risiko yang dapat ditolerir	Tidak / Iya			Hasil evaluasi risiko	Setelah evaluasi	Rencana penanganan risiko	
6	Menentukan dan menerapkan tindakan penanganan risiko				Rencana penanganan risiko	Berdasarkan kebutuhan	Risiko-risiko terkendali	
7	Memantau efektifitas dari tindakan penanganan risiko				Laporan penanganan risiko	Secara berkala	Laporan hasil pemantauan	
8	Menyusun dan melaporkan hasil dari manajemen risiko				Dokumen manajemen risiko	Secara berkala	Laporan manajemen risiko	

Lampiran 2. SOP manajemen risiko

IDENTITAS DOKUMEN

Section	Keterangan
Nama Dokumen	Standar Manajemen Risiko MySMAMITA
Institusi	SMA Muhammadiyah 1 Taman Sidoarjo
Unit Terkait	Tim IT, Admin MySMAMITA dan Guru/walikelas
Pengelola Risiko	Tim IT MySMAMITA
Acuan	ISO 31000:2018 Manajemen Risiko
Versi	1.0
Tanggal Berlaku	20 Desember 2025
Disahkan Oleh	Kepala SMA Muhammadiyah 1 Taman

BAB 1

PENDAHULUAN

1.1 Umum

Pemanfaatan Sistem Absensi MySMAMITA di SMA Muhammadiyah 1 Taman mempunyai urgensi dalam mendukung pengelolaan data kehadiran peserta didik secara efisien. Sebagai bagian dari upaya peningkatan tata kelola absensi di SMA Muhammadiyah 1 Taman, diperlukan suatu standar manajemen risiko sebagai pedoman resmi dalam mengelola risiko yang mungkin dalam penggunaan Sistem Absensi MySMAMITA.

1.2 Maksud dan Tujuan

1.2.1 Maksud

Maksud disusunnya standar manajemen risiko ini yakni untuk dijadikan pedoman bagi semua yang terlibat di SMA Muhammadiyah 1 Taman dalam penerapan pengelolaan risiko Sistem Absensi MySMAMITA secara terstruktur.

1.2.2 Tujuan

Tujuan disusunnya standar manajemen risiko berikut antara lain:

1. Memberikan pemahaman yang seragam mengenai pengelolaan risiko dalam penggunaan Sistem Absensi MySMAMITA.
2. Mengidentifikasi dan menilai potensi risiko yang dapat mempengaruhi kualitas dan keandalan data absensi.

Lampiran 3. Standar Risiko bab I

3. Menetapkan kerangka dan arah pengendalian risiko yang efektif.
4. Mendukung peningkatan mutu layanan akademik melalui pengelolaan risiko yang terencana dan terdokumentasi.

1.3 Ruang Lingkup

Standar manajemen risiko mencakup prinsip dan kerangka kerja pengelolaan risiko berhubungan dengan Sistem Absensi MySMAMITA. antara lain pendekatan identifikasi risiko, menganalisis dan mengevaluasi risiko, penetapan dan pengendalian risiko, monitoring dan review risiko secara berkala serta dokumentasi dan pelaporan hasil dari pengelolaan risiko.

1.4 Dasar Hukum

Penyusunan standar manajemen risiko ini berdasar atas prinsip manajemen risiko yang diatur dalam ISO 31000:2018 *Risk Management - Guidelines*, sebagai standar internasional pedoman prinsip, kerangka kerja serta proses dalam oenerapan manajemen risiko oeganisasi. (ISO/TC262, 2018) (Dr. Antonius Alijoyo, 2018).

Lampiran 4. Standar Risiko Bab I bag. 2

BAB II

STRUKTUR MANAJEMEN RISIKO

Manajemen risiko dalam pengoperasian Sistem Absensi MySMAMITA dilakukan melalui struktur manajemen risiko yang ditetapkan oleh Kepala SMA Muhammadiyah 1 Taman. Struktur ini mengikuti prinsip integrasi manajemen risiko dalam semua tingkatan dan fungsi organisasi, seperti yang ditekankan dalam ISO 31000:2018. Antonius menyatakan bahwa manajemen risiko harus terkait langsung dengan semua aktivitas organisasi agar pengendaliannya berjalan efektif (Dr. Antonius Alijoyo, 2018). Tujuan dari struktur ini adalah memastikan manajemen risiko berjalan secara terarah, terkoordinasi, dan sejalan dengan pelaksanaan SOP Manajemen Risiko MySMAMITA.

Struktur Manajemen Risiko MySMAMITA terdiri dari beberapa komponen, yaitu:

1. Penanggung Jawab Manajemen Risiko

Penanggung jawab manajemen risiko (Tim IT) bertugas menetapkan kebijakan, memberikan arahan, serta memantau secara umum pelaksanaan manajemen risiko MySMAMITA.

2. Pengelola Manajemen Risiko (Risk Owner)

Pengelola manajemen risiko (admin MySMAMITA) bertanggung jawab sebagai pemilik risiko dalam pengelolaan Sistem Absensi MySMAMITA. *risk owner* mengkoordinasikan proses identifikasi, analisis, evaluasi, dan pengendalian risiko sesuai standar yang ditetapkan.

3. Pelaksana Manajemen Risiko

Pelaksana manajemen risiko adalah guru atau walikelas yang berperan dalam mendukung pelaksanaan manajemen risiko secara operasional sesuai dengan SOP yang berlaku. Tugas nya mengidentifikasi risiko yang mungkin terjadi dalam penggunaan sistem serta melaporkan masalah yang ditemukan.

4. Pengawasan dan Evaluasi Manajemen Risiko

Pengawasan dan evaluasi manajemen risiko dilakukan oleh Kepala Sekolah dan Admin MySMAMITA/Tim IT untuk memastikan bahwa pengendalian risiko berjalan efektif, sesuai standar, dan sesuai dengan SOP yang berlaku.

Struktur Manajemen Risiko MySMAMITA bersifat dinamis dan bisa disesuaikan sesuai kebutuhan sekolah serta perkembangan Sistem Absensi MySMAMITA. Perlu adanya penyesuaian jika terjadi perubahan kebijakan sekolah, sistem, atau proses pengelolaan data akademik.

Lampiran 5. Standar Risiko Bab II

BAB III

KERANGKA DAN PROSES MANAJEMEN RISIKO

3.1 Kerangka Manajemen Risiko

Kerangka manajemen risiko dalam pengelolaan Sistem Absensi MySMAMITA memastikan bahwa pengelolaan risiko dilakukan secara terstruktur, dan konsisten dengan tujuan organisasi sekolah. Kerangka manajemen risiko MySMAMITA mencakup komitmen pimpinan sekolah, penetapan peran dan tanggung jawab, integrasi manajemen risiko ke dalam kebijakan dan SOP sekolah, serta pemantauan dan peninjauan secara berkala.

3.2 Penetapan Konteks dan Kriteria Risiko

3.2.1 Penetapan Konteks

Penetapan konteks manajemen risiko dilakukan untuk memahami lingkungan internal dan eksternal yang mempengaruhi pengelolaan Sistem Absensi MySMAMITA. Konteks internal meliputi struktur organisasi sekolah, sumber daya manusia, kebijakan internal, serta infrastruktur teknologi informasi. Konteks eksternal mencakup regulasi pendidikan, kebutuhan pemangku kepentingan, serta perkembangan teknologi.

Penetapan konteks ini bertujuan untuk memastikan bahwa risiko yang diidentifikasi relevan dengan kondisi dan tujuan sekolah.

3.2.2 Kriteria Risiko

Kriteria risiko ditetapkan sebagai dasar untuk menilai tingkat risiko dan menentukan prioritas penanganan risiko. Penilaian risiko dilakukan dengan mempertimbangkan tingkat kemungkinan terjadinya risiko dan dampak yang ditimbulkan terhadap pengelolaan Sistem Absensi MySMAMITA.

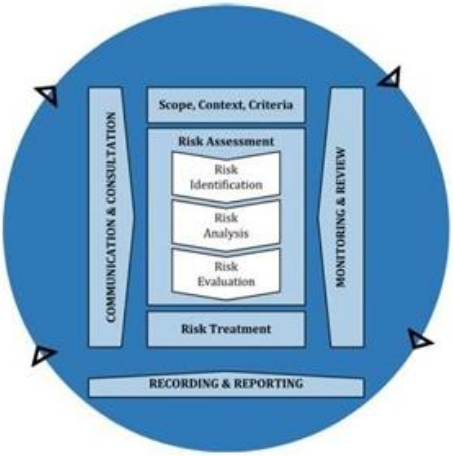
Sekolah menetapkan batas toleransi risiko sebagai berikut:

a. Risiko dengan tingkat rendah dapat diterima karena berdampak minimal
b. Risiko dengan tingkat menengah memerlukan perlakuan risiko sesuai kebijakan yang ditetapkan dan monitoring berkala karena masih dapat ditoleransi
c. Risiko dengan tingkat tinggi perlu adanya tindakan mitigasi segera dengan prioritas penanganan di bawah level kritis, karena secara dampak yang diberikan juga signifikan bagi sistem
d. Risiko dengan tingkat kritis *(catastrophic)* memberi dampak paling bahaya, sehinga perlu tindakan darurat dan menjadi prioritas tertinggi penanganan.

Lampiran 6. Standar Risiko Bab III

3.3 Proses Manajemen Risiko

Proses manajemen risiko pada Sistem Absensi MySMAMITA dilaksanakan berdasarkan tahapan yang mengacu pada ISO 31000:2018, yaitu komunikasi dan konsultasi, identifikasi risiko, analisis risiko, evaluasi risiko, perlakuan risiko, pencatatan dan pelaporan, serta monitoring dan review.



Gambar 1 Proses manajemen risiko

3.3.1 Komunikasi dan Konsultasi

Komunikasi dan konsultasi dilakukan dengan melibatkan pihak-pihak terkait, seperti Tim IT MySMAMITA, admin sistem, serta pengguna sistem. Tujuan dari tahap ini adalah untuk mendukung pemahaman mengenai kondisi sistem, permasalahan yang pernah terjadi, dan potensi risiko yang mungkin muncul.

3.3.2 Penetapan Tujuan dan Konteks

Penetapan tujuan, ruang lingkup, dan konteks merupakan tahapan awal dalam proses manajemen risiko MySMAMITA. Pada tahap ini, sekolah menetapkan tujuan pengelolaan risiko serta memastikan bahwa konteks dan kriteria risiko yang digunakan mengacu pada ketentuan yang telah ditetapkan pada Subbab 3.2.

Lampiran 7. Standar Risiko Bab III bag. 2

3.3.3 Penilaian Risiko

Identifikasi risiko merupakan bagian dari tahapan penilaian risiko yang mencakup identifikasi risiko, analisis risiko, dan evaluasi risiko (Setiawan, Sekarini, Waluyo & Afiana, 2021).

3.3.3.1 Identifikasi Risiko

Identifikasi risiko dilakukan untuk mengenali potensi kejadian yang dapat menghambat pencapaian tujuan pengelolaan Sistem Absesni MySMAMITA. Risiko dapat bersumber dari faktor manusia, proses, teknologi, maupun lingkungan organisasi

3.3.3.2 Analisis Risiko

Risiko yang telah diidentifikasi dianalisis untuk menentukan tingkat kemungkinan terjadinya dan dampak yang ditimbulkan. Hasil analisis digunakan untuk mengetahui tingkat risiko yang dihadapi oleh sistem (Setiawan, Sekarini, Waluyo & Afiana, 2021).

3.3.3.3 Evaluasi Risiko

Evaluasi risiko dilakukan untuk menentukan prioritas risiko yang perlu ditangani. Risiko dengan tingkat menengah dan tinggi menjadi prioritas utama dalam perlakuan risiko.

3.3.4 Perlakuan Risiko

Perlakuan risiko dilakukan dengan menentukan strategi penanganan risiko yang sesuai. Strategi perlakuan risiko dapat berupa pengurangan risiko, penghindaran risiko, pemindahan risiko, atau penerimaan risiko sesuai dengan tingkat risiko dan kemampuan sekolah dalam mengelola risiko tersebut.

3.3.5 Pencatatan dan Laporan

Pencatatan dan pelaporan dilakukan untuk mendokumentasikan seluruh proses manajemen risiko MySMAMITA, mulai dari hasil identifikasi risiko, analisis risiko, evaluasi risiko, hingga keputusan perlakuan risiko. Dokumentasi ini digunakan sebagai dasar pengambilan keputusan manajemen, evaluasi efektivitas pengelolaan risiko, serta perbaikan kebijakan dan SOP terkait.

3.3.6 Monitoring dan Review

Monitoring dan review dilakukan secara berkala untuk memastikan efektivitas penerapan manajemen risiko dan kesesuaiannya dengan perubahan kondisi sistem dan lingkungan organisasi. Hasil monitoring dan review digunakan sebagai dasar perbaikan berkelanjutan terhadap pengelolaan risiko MySMAMITA.

Lampiran 8. Standar Risiko Bab III bag. 3

BAB IV

PENERAPAN STANDAR MANAJEMEN RISIKO

4.1 Penerapan Standar Manajemen Risiko

Standar Manajemen Risiko Sistem Absensi MySMAMITA digunakan sebagai pedoman dalam mengelola risiko yang berkaitan dengan penggunaan dan pengelolaan data absensi siswa di SMA Muhammadiyah 1 Taman. Tujuan nya untuk memastikan pengelolaan risiko dilakukan secara terarah, dan sesuai dengan kebijakan sekolah.

Standar ini diterapkan dengan mengintegrasikannya ke dalam kebijakan sekolah dan SOP terkait pengelolaan Sistem Absensi MySMAMITA. Semua pihak yang terlibat dalam penggunaan dan pengelolaan sistem wajib memahami serta mematuhi ketentuan yang terdapat dalam standar ini.

4.2 Keterkaitan Standar Manajemen Risiko dengan SOP

Standar Manajemen Risiko berfungsi sebagai dokumen utama yang menjadi dasar dalam penyusunan dan penerapan SOP Manajemen Risiko serta SOP Pengelolaan Sistem Absensi MySMAMITA.

SOP disusun sebagai panduan dalam pelaksanaan proses manajemen risiko secara teknis dan rinci. Aturan terkait cara mengelola risiko, termasuk pembagian tugas, alur kerja, dan mekanisme pengendalian risiko, diatur lebih lanjut dalam SOP yang berlaku, sesuai dengan kebutuhan operasional sekolah.

4.3 Mandat dan Komitmen Manajemen Sekolah

Mandat dan komitmen dari manajemen sekolah membantu dalam implementasi standar manajemen risiko yang memastikan pengelolaan risiko berjalan berkelanjutan dan efektif. Dengan konteks tersebut, manajemen sekolah mempunya komitmen dalam ;

a. Menetapkan kebijakan manajemen risiko atas data absensi yang dikelola
b. SDM yang diperlukan dipastikan ketersediaanya, mulai dari SDM, dana bahkan teknologinya
c. Komunikasi akan pentingnya manajemen risiko atas seluruh stakeholder terlibat
d. Peran dan tanggungjawab yang jelas terkait pengelolaan risiko

Lampiran 9. Standar Risiko Bab IV

4.4 Implementasi Kerangka Kerja Manajemen Risiko

Implementasi kerangka kerja dengan mengintegrasikan standar manajemen kedalam proses organisasi sekolah yang berhubungan dengan sistem absensi MySMAMITA agar integrasinya membantu dalam pelaksanaan kegiatan operasional dan pengambilan keputuasn. Implementasi teknis kerangka kerja ini dilaksanakan dari SOP yang sudah disusun, yang akan menjadi pedoman operasional saat menjalankan proses manajemen risiko berdasar standar yang telah ditentukan (Nasional, 2016).

4.5 Pemantauan dan Perbaikan Berkelanjutan

Dalam memastikan efektivitas dari implementasi standar risiko, sekolaj perlu melaksanakan tinjauan secara berkala dengan tujuan agar dapat menilai kesesuaian kondisi sistem dengan penerapan standar risiko nya (Nasional, 2016). Melalui hasil pemantauan dan tinjauan, perbaikan berkelanjutan terhadap standar risiko, SOP dan kebijakan dilakukan oleh sekolah agar sesuai dengan kebutuhan sistem absensi MySMAMITA.

Lampiran 10. Standar Risiko Bab IV bag. 2

BAB V

PENUTUP

Standar Manajemen Risiko Sistem Absensi MySMAMITA ini dibuat sebagai panduan utama dalam mengelola risiko secara teratur dan berkelanjutan. Standar ini menjadi dasar dalam membuat dan menerapkan SOP Manajemen Risiko yang digunakan sehari-hari. Standar ini diharapkan bisa menjadi pedoman bagi semua pihak yang terlibat dalam menjaga sistem absensi yang handal, aman, dan berkelanjutan.

Dengan adanya standar manajemen risiko ini, sekolah menunjukkan komitmen untuk mengelola risiko secara terstruktur dan konsisten melalui kebijakan serta SOP yang sudah ditetapkan. Penerapan standar ini diharapkan bisa mengurangi risiko yang mungkin terjadi, meningkatkan kualitas pengelolaan data absensi, serta membantu meningkatkan kualitas layanan pendidikan. Standar Manajemen Risiko ini akan diperiksa dan diperbaiki secara berkala sesuai dengan perkembangan sistem, kebutuhan sekolah, serta perubahan lingkungan kerja.

Lampiran 11. Standar Risiko Bab V Penutup