ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA BAGIAN TATA USAHA MENGGUNAKAN FRAMEWORK ISO 31000 PADA MI AL-BAROKAH PAMEUNGPEUK

Alif Febrianto[1], Elin Rosliani[2]
[1]Sistem Informasi Institut Pendidikan Indonesia
[2]Institut Pendidikan Indonesia
[1]aliffebrianto1933@gmail.com, [2]elinrosliani@institutpendidikan.ac.id

ABSTRACT

The rapid growth of information technology (IT) currently demands educational institutions, including elementary schools and madrasahs, to optimize the use of digital systems to enhance the efficiency of school administration (TU) operations. However, the implementation of this technology also introduces various potential risks that can threaten data integrity and the smoothness of school administrative services. This study aims to identify IT risk threats, evaluate risk levels, and develop mitigation strategy recommendations for the Administration Department at MI Al-Barokah Pameungpeuk, Garut. The method used in this research is a descriptive qualitative approach by applying the international standard risk management framework ISO 31000:2018. Data collection was conducted through direct observation of IT assets and in-depth interviews with the school administration staff. Based on the risk assessment process, the results successfully identified critical asset components and mapped potential IT risk threats, which are classified into three levels: high risk, medium risk, and low risk, based on the multiplication matrix of likelihood and impact values. The final outcome of this research provides structured and adaptive risk treatment recommendations for the management of MI Al-Barokah to minimize daily operational technical disruptions, strengthen information data security, and improve institutional governance preparedness in the future.

Keywords: Risk Analysis, ISO 31000:2018, Risk Management, School Administration, Madrasah.

ABSTRAK

Pesatnya perkembangan teknologi informasi (TI) saat ini menuntut institusi pendidikan, termasuk pada tingkat sekolah dasar dan madrasah, untuk mengoptimalkan pemanfaatan sistem digital guna meningkatkan efisiensi operasional tata usaha (TU). Namun, implementasi teknologi ini juga membawa berbagai potensi risiko yang dapat mengancam integritas data dan kelancaran layanan administrasi sekolah. Penelitian ini bertujuan untuk mengidentifikasi ancaman risiko TI, mengevaluasi tingkat risiko, serta menyusun rekomendasi strategi mitigasi pada bagian Tata Usaha MI Al-Barokah Pameungpeuk, Garut. Metode yang digunakan dalam penelitian ini adalah pendekatan kualitatif deskriptif dengan menerapkan kerangka kerja manajemen risiko standar internasional ISO 31000:2018. Pengumpulan data dilakukan melalui observasi langsung pada aset TI dan wawancara mendalam bersama staf tata usaha sekolah. Berdasarkan proses penilaian risiko (*risk assessment*), hasil penelitian berhasil mengidentifikasi komponen aset penting serta memetakan potensi ancaman risiko TI yang diklasifikasikan ke dalam tiga tingkatan, yaitu tingkat risiko tinggi (*high risk*), risiko sedang (*medium risk*), dan risiko rendah (*low risk*) berdasarkan matriks perkalian nilai kemungkinan (*likelihood*) dan dampak (*impact*). Hasil akhir dari penelitian ini memberikan usulan tindakan penanganan risiko (*risk treatment*) yang terstruktur dan adaptif bagi pihak manajemen MI Al-Barokah guna meminimalisir gangguan teknis operasional harian, memperkuat keamanan data informasi, serta meningkatkan kesiapan tata kelola institusi di masa mendatang.

Kata Kunci: Analisis Risiko, ISO 31000:2018, Manajemen Risiko, Tata Usaha, Madrasah.

A. Pendahuluan

Perkembangan teknologi informasi (TI) pada era digital saat ini telah merambah ke berbagai sektor operasional institusi, termasuk di dalamnya adalah lembaga pendidikan formal tingkat dasar seperti Madrasah Ibtidaiyah (MI). Transformasi dari tata kelola konvensional menuju sistem digital dinilai sangat vital guna mendongkrak efisiensi, akurasi data, serta efektivitas pelayanan administrasi pada bagian Tata Usaha (TU). Keberhasilan integrasi teknologi

ini mampu mempermudah pengolahan data kepegawaian, arsip kesiswaan, dan pelaporan berkala secara dinamis. Namun demikian, akselerasi adopsi TI pada lingkungan sekolah dasar negeri maupun swasta juga membawa konsekuensi tersendiri berupa munculnya kerentanan teknis dan ancaman baru. Kendala mendasar seperti rendahnya literasi digital staf pengguna, keterbatasan fasilitas infrastruktur penunjang, serta kerentanan sistem terhadap gangguan teknis harian menjadi faktor penghambat utama yang sering dihadapi oleh instansi pendidikan (Pusparani & Nayla, 2025).

Tantangan operasional TI ini secara nyata juga dihadapi oleh MI Al-Barokah Pameungpeuk Garut, khususnya pada bagian unit kerja Tata Usaha. Berdasarkan hasil pengamatan awal, aktivitas administrasi di madrasah ini sudah mulai memanfaatkan sistem informasi digital, baik untuk kebutuhan data internal maupun pelaporan eksternal ke kementerian terkait. Kendati sangat membantu tugas rutin staf, sistem elektronik yang berjalan kerap dihadapkan pada potensi ancaman. Risiko kehilangan database akibat kerusakan perangkat keras, ancaman infeksi malware, hingga potensi terjadinya *human error* pada proses *input* data kesiswaan harian menjadi tantangan utama yang harus dihadapi (H, Nasrullah, & Kusumawati, 2025). Selain itu, masalah teknis seperti server yang sering down atau koneksi jaringan yang mendadak terputus juga berpotensi mengganggu efisiensi jalannya pelayanan administrasi secara real-time (Kanantyo & Papilaya, 2021). Kondisi tersebut apabila dibiarkan tanpa adanya pengelolaan yang terstruktur dapat menghambat jalannya proses bisnis lembaga secara keseluruhan.

Guna memastikan seluruh aset TI dan keberlangsungan operasional di MI Al-Barokah tetap terjaga dengan aman, penerapan sebuah mekanisme tata kelola risiko yang terstandarisasi menjadi instrumen yang sangat mendesak untuk diterapkan. Manajemen risiko TI yang efektif sangat penting untuk memaksimalkan kegunaan aset teknologi informasi dan meningkatkan efisiensi proses bisnis (Yolanda, 2024). Melalui pendekatan manajemen risiko yang tepat, sekolah dapat mengantisipasi ancaman sedini mungkin serta

mengurangi dampak kerugian yang mungkin ditimbulkan terhadap proses pelayanan administrasi akademik (Joice, Br, Tanaamah, & Muttamaqin, 2026). Dengan memetakan potensi ancaman sejak awal, pihak manajemen sekolah dapat mengambil keputusan yang tepat untuk meminimalkan gangguan teknis operasional harian berdasarkan skala prioritas penanganan risiko yang paling kritis.

Salah satu metodologi manajemen risiko yang paling adaptif, fleksibel, dan diakui secara internasional untuk diterapkan pada berbagai skala organisasi adalah *framework* ISO 31000. Standar ISO 31000 menyediakan panduan kerangka kerja yang komprehensif mulai dari penentuan ruang lingkup kriteria, identifikasi ancaman, analisis risiko, evaluasi tingkatan risiko, hingga penyusunan usulan strategi perlakuan (*risk treatment*). Implementasi model kerangka kerja ini terbukti sangat efektif untuk mengidentifikasi risiko operasional utama pada sistem informasi serta memberikan rekomendasi strategi mitigasi yang sesuai (Pusparani & Nayla, 2025). Berdasarkan latar belakang problematika tersebut, penelitian artikel ilmiah ini dilakukan dengan judul "Analisis Manajemen Risiko Teknologi Informasi pada Bagian Tata Usaha Menggunakan Framework ISO 31000 (Studi Kasus: MI Al-Barokah Pameungpeuk)". Penelitian ini diharapkan dapat menghasilkan usulan tindakan penanganan risiko yang terstruktur dan adaptif bagi pihak madrasah guna meningkatkan kesiapan tata kelola institusi di masa mendatang (Joice et al., 2026).

B. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan menerapkan metode penelitian studi kasus (*case study research*). Pemilihan metode studi kasus ini bertujuan agar peneliti dapat berfokus penuh pada satu objek penelitian secara mendalam, sehingga seluruh data primer dan informasi valid yang berkaitan dengan manajemen risiko teknologi informasi dapat dikumpulkan secara lebih terpusat. Kerangka kerja utama yang diterapkan dalam penelitian ini merujuk pada standar manajemen risiko internasional ISO 31000:2018. *Framework* ini dipilih karena

memberikan pendekatan yang lebih sistematis, terstruktur, strategis, serta mudah diimplementasikan pada berbagai skala tata kelola organisasi instansi pendidikan.

1. Metode Pengumpulan Data

Proses pengumpulan data primer dan sekunder dalam penelitian ini dilaksanakan melalui tiga tahapan terintegrasi guna menjamin validitas informasi yang diperoleh:

a. Studi Literatur:

Melakukan tinjauan pustaka terhadap jurnal ilmiah, teori pendukung, dokumen regulasi, serta standar operasional yang relevan dengan penerapan manajemen risiko TI berbasis ISO 31000.

b. Wawancara Mendalam:

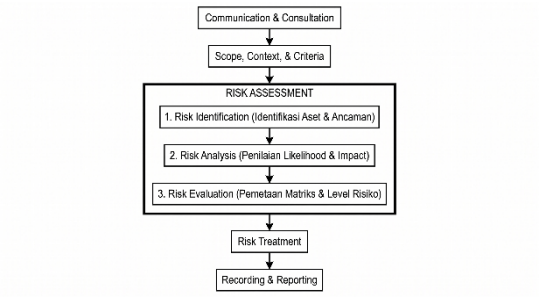
Melakukan tanya jawab secara langsung dengan pemangku kepentingan (*stakeholders*) internal, khususnya kepala madrasah dan staf pelaksana pada bagian unit kerja Tata Usaha (TU) MI Al-Barokah untuk menggali data primer mengenai kendala teknis operasional harian.

c. Observasi Lapangan:

Melakukan pengamatan secara langsung terhadap kondisi fisik, kinerja, tingkat pemanfaatan, serta prosedur keamanan aset-aset TI yang digunakan dalam menunjang layanan administrasi sekolah.

2. Metode Analisis Data

Proses analisis data dalam penelitian ini mengikuti seluruh tahapan yang tertuang di dalam siklus *Risk Management Process* berdasarkan pedoman framework ISO 31000:2018. Merujuk pada standardisasi tersebut, tahapan analisis data dijabarkan sebagai berikut:



Gambar 1. Siklus *Risk Management Process*

a. Communication and Consultation:

Membangun komunikasi awal dengan pihak madrasah untuk menyamakan persepsi mengenai urgensi pelaksanaan evaluasi risiko teknologi informasi.

b. Scope, Context, and Criteria:

Menetapkan batasan ruang lingkup penelitian yang berfokus pada layanan administrasi TU serta merumuskan kriteria penilaian risiko.

c. Risk Assessment:

Tahapan inti yang mencakup tiga sub-proses utama, yaitu:

1. *Risk Identification:*

Mengidentifikasi seluruh komponen aset TI (data, *software*, *hardware*) serta mengungkap berbagai potensi ancaman risiko yang dapat muncul pada aktivitas bisnis TU.

2. *Risk Analysis:*

Menilai tingkat frekuensi terjadinya risiko (*likelihood*) dan bobot keparahan dampaknya (*impact*) menggunakan skala Likert rating 1 sampai 5. Nilai indeks risiko diperoleh melalui rumus standar:

Level Risiko = Likelihood (L) × Impact (I)

3. *Risk Evaluation:*

Membandingkan nilai indeks risiko ke dalam matriks evaluasi risiko untuk mengklasifikasikan status ancaman ke dalam tiga tingkatan level risiko, yaitu *High Risk*, *Medium Risk*, dan *Low Risk*.

d. Risk Treatment:

Menyusun rekomendasi strategi mitigasi atau usulan tindakan penanganan yang konkrit dan adaptif bagi pihak manajemen sekolah untuk meminimalisir kemungkinan terjadinya risiko di masa depan.

e. Recording and Reporting:

Mendokumentasikan seluruh hasil analisis manajemen risiko ke dalam bentuk laporan terstruktur sebagai dokumen referensi tata kelola madrasah.

C.Hasil Penelitian dan Pembahasan

1. Penilaian Risiko (*Risk Assessment*)

Berdasarkan tahapan proses manajemen risiko ISO 31000:2018 yang telah dilaksanakan melalui observasi langsung dan wawancara mendalam bersama pihak manajemen dan staf Tata Usaha (TU) MI Al-Barokah Pameungpeuk, diperoleh rincian hasil analisis yang terstruktur. Proses penilaian risiko ini meliputi tiga tahapan utama, yaitu identifikasi aset beserta ancaman, analisis bobot nilai, dan evaluasi tingkatan risiko.

a. Identifikasi Aset (*Risk Identification*)

Langkah awal dalam mitigasi risiko adalah memetakan seluruh komponen aset Teknologi Informasi (TI) yang digunakan dalam mendukung aktivitas pelayanan administrasi harian di bagian Tata Usaha. Komponen aset TI pada TU MI Al-Barokah dikelompokkan ke dalam tiga kategori utama, yaitu data, *software*, dan

hardware seperti yang tertera pada Tabel 1.

Komponen SI/TI	Aset pada Bagian Tata Usaha MI Al-Barokah
Data	1.Data Induk Siswa (Dapodik / EMIS Kemenag) 2.Arsip Digital Surat Masuk & Keluar 3.Data Rekapitulasi Keuangan & SPP Madrasah
Software	1.Aplikasi EMIS Kemenag & Dapodik 2.Web Browser & Aplikasi Pengolah Kata (Spreadsheet/Excel) 3.Sistem Operasi Perangkat Kerja
Hardware	1.Perangkat Komputer / Laptop Operasional TU 2.Perangkat Infrastruktur Jaringan (Modem & Router Wifi) 3.Media Penyimpanan Eksternal (Flashdisk / Harddisk Eksternal)

b. Identifikasi Kemungkinan Risiko dan Dampak

Setelah seluruh komponen aset TI berhasil dipetakan, langkah berikutnya adalah mengidentifikasi potensi ancaman risiko operasional yang kerap muncul atau rawan terjadi dalam pemanfaatan teknologi di lingkungan madrasah. Seluruh indikator ancaman tersebut beserta penyebab dan dampak negatifnya dirinci pada Tabel 2.

Kategori Faktor	ID	Kemungkinan Risiko	Akar Penyebab	Dampak Konsekuensi
Manusia (SDM)	R01	Kesalahan input data administrasi	Kurangnya ketelitian staf TU atau kebingungan terhadap antar muka aplikasi.	Terjadinya ketidakvalidan laporan dan keterlambatan sinkronisasi data pusat.

	R02	Keterbatasan literasi digital staf	Minimnya pelatihan berkala mengenai operasional sistem administrasi terbaru.	Penggunaan teknologi kurang optimal dan menurunkan produktivitas kerja.
Sistem & Infrastruktur	R03	Koneksi jaringan internet terputus/down	Lokasi geografis dan keterbatasan bandwidth dari penyedia layanan internet lokal.	Proses sinkronisasi EMIS/ Dapodik terhambat dan layanan real-time lumpuh.
	R04	Kehilangan database lokal	Kerusakan pada harddisk komputer operasional akibat usia perangkat.	Kehilangan data-data penting kesiswaan dan biaya pemulihan data yang tinggi.
	R05	Kurangnya backup data rutin	Ketiadaan prosedur standar operasional (SOP) untuk pencadangan data ke cloud.	Risiko kehilangan informasi secara permanen saat perangkat utama eror.

	R06	Infeksi malware / serangan virus	Seringnya penggunaan media penyimpanan eksternal (flashdisk) secara bergantian.	Kerusakan sistem operasi komputer operasional dan risiko data corrupt.
Lingkungan & Alam	R07	Pemadaman listrik tiba-tiba	Pasokan daya listrik PLN yang tidak stabil di wilayah Pameungpeuk Garut.	Sistem mati mendadak, kerusakan hardware, dan hilangnya data yang belum disimpan.

2. Analisis dan Pembahasan Nilai Risiko (*Risk Analysis*)

Proses analisis risiko dilakukan dengan menentukan bobot nilai tingkat frekuensi terjadinya risiko (*likelihood*) dan tingkat keparahan dampak (*impact*). Penilaian didasarkan pada skala indikator 1 sampai 5 melalui konfirmasi kondisi riil di lapangan.

a. Likelihood (Kemungkinan):

Menilai seberapa sering ancaman tersebut muncul dalam kurun waktu operasional tertentu.

b. Impact (Dampak):

Menilai seberapa besar gangguan yang ditimbulkan terhadap keberlangsungan proses pelayanan administrasi madrasah.

Hasil pembobotan nilai serta perhitungan indeks tingkat risiko untuk *(Likelihood × times Impact)* 7 indikator ancaman utama di bagian TU MI Al-Barokah disajikan secara mendalam pada Tabel 3.

ID	Kemungkinan Ancaman Risiko TI	Likelihood (1-5)	Impact (1-5)	Skor Indeks (L × I)	Tingkat Level Risiko (Ris

					k Level)
R03	Koneksi jaringan internet terputus/down	4	4	16	High (Tinggi)
R07	Pemadaman listrik tiba-tiba	4	4	16	High (Tinggi)
R01	Kesalahan input data administrasi	3	3	9	Medium (Sedang)
R04	Kehilangan database lokal	2	4	8	Medium (Sedang)
R05	Kurangnya backup	3	3	9	Medium (Se
	p data rutin				dang)
R06	Infeksi malware / serangan virus	3	3	9	Medium (Sedang)
R02	Keterbatasan literasi digital staf	2	3	6	Low (Rendah)

3. Perlakuan Risiko (*Risk Treatment*)

Berdasarkan hasil pemetaan tingkat level risiko pada Tabel 3, disusun usulan rekomendasi strategi mitigasi (*risk treatment*) yang konkrit, adaptif, dan efisien untuk diterapkan oleh pihak manajemen MI Al-Barokah Pameungpeuk guna meminimalisir dampak ancaman di masa mendatang seperti pada Tabel 4.

ID	Risiko TI	Risk Level	Usulan Tindakan Penanganan / Mitigasi Risiko
R03	Koneksi jaringan	High	Menyediakan koneksi

	internet terputus/ down		internet cadangan via modem seluler (multi-ISP) guna mengantisi pasi kegagalan jaringan utama saat deadline pelaporan.
R 07	Pemada man listrik tiba-tiba	High	Menyediak an perangkat Uninterrupti ble Power Supply (UPS) pada komputer operasional utama TU agar staf memiliki waktu menyimpan data saat listrik padam.
R 01	Kesalaha n input	Medi um	Menerapka n prosedur

	data administr asi		validasi bertingkat sebelum data disinkronisa si ke aplikasi pusat serta pembuatan formulir input yang lebih ringkas.
R 04	Kehilang an database lokal	Medi um	Melakukan peremajaan komponen penyimpan an hardware secara berkala serta membatasi akses penggunaa n laptop operasional untuk urusan non-dinas.
R 05	Kurangn ya	Medi um	Menyusun SOP

	backup data rutin		tertulis wajib bagi staf TU untuk melakukan pencadangan data (backup) otomatis ke local server cloud (Google Drive) setiap akhir pekan.
R 06	Infeksi malware / serangan virus	Medium	Memasang anti-virus resmi yang selalu diperbarui, mengaktifkan fitur firewall bawaan, serta membatasi plug-and-play media penyimpanan eksternal asing.
R 02	Keterbatasan literasi digital staf	Low	Mengikutsertakan staf administrasi ke dalam pelatihan atau bimtek teknologi informasi dasar secara internal maupun eksternal.

D. Kesimpulan

Berdasarkan hasil analisis manajemen risiko teknologi informasi yang telah dilaksanakan pada bagian Tata Usaha (TU) MI Al-Barokah Pameungpeuk Garut dengan menerapkan *framework* ISO 31000:2018, diperoleh beberapa kesimpulan mendasar mengenai kondisi tata kelola risiko di madrasah tersebut. Melalui tahapan identifikasi yang sistematis, penelitian ini berhasil mengungkap tujuh indikator ancaman utama yang memengaruhi operasional administrasi sekolah, di mana seluruh ancaman tersebut dikelompokkan ke dalam tiga kategori faktor, yaitu faktor manusia (SDM),

faktor sistem dan infrastruktur, serta faktor lingkungan dan alam. Hasil evaluasi tingkat risiko menunjukkan adanya dua ancaman kritis yang menduduki kategori tingkat tinggi (*High Risk*) dengan nilai skor indeks mencapai 16, yaitu kendala konektivitas jaringan internet yang sering terputus atau *down* serta masalah pemadaman arus listrik PLN secara tiba-tiba di wilayah Pameungpeuk Garut. Sementara itu, empat indikator lainnya masuk ke dalam kategori tingkat sedang (*Medium Risk*) yang meliputi kesalahan *input* data kesiswaan oleh staf, risiko kehilangan database lokal akibat kerusakan *harddisk*, kurangnya aktivitas *backup* data secara rutin, dan ancaman infeksi malware dari media penyimpanan eksternal. Adapun satu indikator terakhir berada pada tingkatan risiko rendah (*Low Risk*), yaitu keterbatasan literasi digital yang dimiliki oleh staf pelaksana tata usaha. Secara keseluruhan, penerapan model standar internasional ISO 31000:2018 ini terbukti mampu menyediakan kerangka kerja yang sangat terstruktur dan adaptif bagi manajemen MI Al-Barokah untuk mendeteksi kelemahan infrastruktur digital sejak dini, sehingga penentuan kebijakan mitigasi dapat diambil secara tepat dan efisien berdasarkan skala prioritas ancaman yang paling berdampak buruk bagi organisasi.

DAFTAR PUSTAKA

Jurnal :

H, B. Y. F. A., Nasrullah, M., & Kusumawati, A. (2025). Analisis Manajemen Risiko dengan Menggunakan Framework ISO 31000 : 2018 pada Sistem Informasi E-Gudang Satpol PP Kota Surabaya Risk Management Analysis Using the ISO 31000 : 2018 Framework on the E-Gudang Information System of the Civil Service Police Uni, 79–91.

Joice, H., Br, I., Tanaamah, A. R., & Muttamaqin, A. (2026). Analisis manajemen risiko pada e-learning SMAN 1 Ambarawa dengan menggunakan ISO 31000 : 2018, *23*(1), 1–13. https://doi.org/10.24246/aiti.v23i1.1-13

Kanantyo & Papilaya. (2021). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (, *8*(4).

Pusparani, A., & Nayla, A. (2025). Analisis Risiko Penggunaan E-Kinerja pada Kalangan Pegawai Negeri Sipil di SMA Negeri 1 Toboali Menggunakan Framework Iso 31000, *06*(01), 93–106.