Jurnal Penelitian Nusantara
Volume 2 ; Nomor 6 ; Juni 2026 ; Page 98-104
Doi : https://doi.org/10.59435/menulis.v2i6.1180
Website : https://padangjurnal.web.id/index.php/menulis
E-ISSN : 3088-988X

Manajemen Risiko Sistem Informasi Akademik Universitas XYZ Menggunakan Metode ISO 31000

Ardiansyah Hidayat[1*], Muhammad Fidel Salim[2]

[1] Fakultas Ilmu Komputer, Universitas Muslim Indonesia
[2] Fakultas Ilmu Komputer, Universitas Muslim Indonesia
[1]*13020230002@umi.ac.id, [2]13020230006@umi.ac.id

Abstrak

Pengelolaan data melalui Sistem Informasi Akademik (SIAKAD) di perguruan tinggi memiliki kerentanan terhadap ancaman keamanan dan kegagalan operasional. Penelitian ini bertujuan untuk mengidentifikasi, mengevaluasi, dan memitigasi risiko pada pengelolaan data akademik di Fakultas Ilmu Komputer Universitas XYZ menggunakan standar keamanan ISO 31000:2018. Masalah utama yang diteliti mencakup ancaman akses ilegal, penipuan (*phishing*), kelalaian pengguna, kesalahan fungsionalitas, hingga gangguan peladen (*server down*). Metode yang digunakan adalah semi-kuantitatif melalui kuesioner kepada mahasiswa sebagai pengguna akhir guna memetakan frekuensi dan dampak risiko. Hasil penelitian menunjukkan bahwa dari 5 risiko utama yang dievaluasi, sebesar 20% (1 risiko) berada pada level Tinggi yaitu *Bug/Error* fungsionalitas sistem yang menuntut penanganan prioritas. Sementara itu, 80% (4 risiko) lainnya berada pada level Sedang. Sebagai solusi penyelesaian, dirumuskan strategi perlakuan risiko yang meliputi mitigasi teknis berupa audit sistem dan kebijakan wajib kata sandi kuat, pembagian risiko melalui penyewaan *cloud hosting* saat masa pengisian rencana studi, serta penerimaan risiko yang diimbangi dengan edukasi keamanan siber. Penerapan solusi ini diharapkan mampu menjamin ketersediaan dan integritas layanan akademik secara berkelanjutan.

Kata Kunci: Manajemen Risiko, ISO 31000, Sistem Informasi Akademik, Keamanan Data.

PENDAHULUAN

Di era transformasi digital saat ini, perguruan tinggi khususnya Fakultas Ilmu Komputer Universitas XYZ, telah menempatkan teknologi informasi sebagai pilar utama dalam penyelenggaraan pendidikan. Ketergantungan yang tinggi terhadap *Sistem Informasi Akademik* (SIAKAD) menjadi hal yang tidak terelakkan, mengingat sistem ini mengintegrasikan seluruh lini kegiatan akademik mulai dari pengisian *Kartu Rencana Studi* (KRS), pengolahan nilai, penjadwalan kuliah, hingga manajemen basis data mahasiswa. Namun, ketergantungan tersebut juga membawa potensi risiko teknologi informasi yang dapat melumpuhkan operasional pendidikan apabila tidak dikelola dengan mitigasi yang tepat. Sistem informasi akademik di perguruan tinggi memiliki potensi ancaman yang perlu diantisipasi, mencakup berbagai kemungkinan risiko yang dapat mengganggu kelancaran proses akademik apabila tidak dikelola dengan baik (Ardius et al., 2025). Risiko pada SIAKAD tidak hanya bersumber dari ancaman eksternal, tetapi juga dari dalam ekosistem kampus itu sendiri, mencakup akses ilegal (*Brute Force*), rekayasa sosial (*Phishing*), kesalahan fungsionalitas sistem (*Bug/Error*), gangguan ketersediaan layanan (*Server Down*), serta kesalahan manusia (*Human Error*).

Penelitian sebelumnya yang dilakukan di lingkungan perguruan tinggi terkait oleh(Kurniati et al., 2019) Sejalan dengan hal tersebut, upaya pengelolaan risiko secara sistematis menjadi solusi yang relevan untuk menjamin keberlangsungan layanan akademik. Solusi yang ditawarkan dalam penelitian ini adalah penerapan kerangka kerja manajemen risiko berdasarkan standar *ISO 31000:2018*, yang mencakup proses identifikasi, analisis, evaluasi, hingga perlakuan risiko secara terstruktur dan berkelanjutan.

Beberapa penelitian terdahulu telah mengkaji penerapan manajemen risiko pada sistem informasi akademik di lingkungan perguruan tinggi. (Nikmat, 2024) melakukan analisis manajemen risiko teknologi informasi pada SIAK Universitas Muhammadiyah Sukabumi menggunakan ISO 31000 dan menemukan bahwa ancaman seperti gangguan koneksi internet, kesalahan penggunaan perangkat lunak, serta kehilangan dokumen merupakan risiko prioritas tinggi yang berpotensi menghambat keberlangsungan proses akademik. (Lubis et al., 2023) mengkaji risiko pada aplikasi registrasi perkuliahan di lingkungan universitas menggunakan kerangka ISO 31000 dan mengidentifikasi bahwa ancaman akses tidak sah, kebocoran data, serta kejahatan siber (*cybercrime*) merupakan risiko tertinggi yang memerlukan penanganan segera melalui penguatan kebijakan kata sandi, enkripsi data, dan edukasi keamanan siber kepada mahasiswa. Sementara itu, (Nadiya et al., 2024) menganalisis risiko sistem informasi akademik menyimpulkan bahwa risiko *server down* serta kebocoran hak akses merupakan ancaman dominan dengan probabilitas tinggi yang perlu diatasi melalui pendekatan mitigasi terstruktur. (Marlando et al., 2025) melakukan penilaian risiko berbasis ISO 31000:2018 pada unit TIK Politeknik Negeri Lampung dan menemukan bahwa profil risiko TI di institusi pendidikan tinggi didominasi oleh risiko level menengah yang membutuhkan pemantauan berkala. Meskipun demikian, keempat penelitian tersebut

memiliki kesamaan keterbatasan, yakni pengumpulan data dilakukan melalui wawancara dengan staf teknis atau pengelola sistem, sehingga perspektif mahasiswa sebagai pengguna akhir (*end-user*) yang paling terdampak langsung belum terwakili secara memadai dalam proses penilaian risiko operasional.

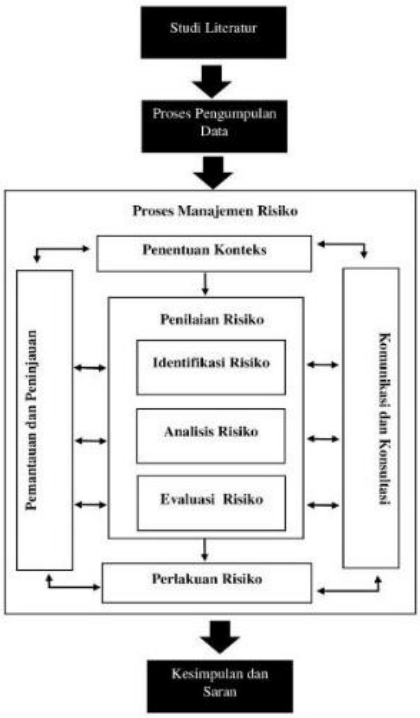
Berdasarkan kajian terhadap penelitian-penelitian terdahulu tersebut, terdapat kesenjangan (*gap*) yang dapat diidentifikasi, yakni belum adanya penelitian yang secara spesifik mengkaji manajemen risiko SIAKAD dari perspektif pengalaman pengguna akhir di lingkungan perguruan tinggi berbasis teknologi seperti FIKOM Universitas XYZ. Penelitian terdahulu umumnya berfokus pada aspek teknis infrastruktur atau melibatkan staf pengelola sistem sebagai sumber data utama, tanpa melibatkan mahasiswa secara langsung sebagai responden dalam penilaian risiko operasional. Perbedaan pendekatan inilah yang menjadi kebaruan dari penelitian ini dibandingkan dengan studi-studi sebelumnya.

Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko operasional pada SIAKAD FIKOM Universitas XYZ menggunakan kerangka kerja *ISO 31000:2018*, dengan pendekatan berbasis pengalaman pengguna akhir melalui instrumen kuesioner yang disebarkan kepada mahasiswa. Hasil penelitian ini diharapkan dapat memberikan rekomendasi pengendalian risiko yang praktis dan aplikatif, sehingga mampu meningkatkan keandalan layanan, melindungi privasi data mahasiswa, serta menjaga integritas akademik FIKOM Universitas XYZ secara berkelanjutan.

METODE

Tahapan Penelitian

Penelitian ini menggunakan kerangka kerja *ISO 31000:2018* sebagai pendekatan sistematis dalam menganalisis dan mengevaluasi risiko operasional pada SIAKAD FIKOM Universitas XYZ. Tahapan penelitian secara keseluruhan dapat dilihat pada Gambar 1.



Gambar 1.Tahapan Penelitian

Penelitian diawali dengan studi literatur untuk memperoleh landasan teoritis yang relevan, mencakup konsep manajemen risiko, kerangka kerja *ISO 31000:2018*, serta penelitian-penelitian terdahulu yang sejenis. Selanjutnya dilakukan proses pengumpulan data melalui penyebaran kuesioner kepada seluruh mahasiswa aktif FIKOM Universitas XYZ angkatan 2022–2025 yang menggunakan SIAKAD, dengan total 23 responden yang berhasil mengisi kuesioner selama periode pengumpulan data. Instrumen kuesioner dirancang untuk mengukur dua dimensi utama pada setiap risiko, yakni dimensi *Likelihood* (tingkat frekuensi terjadinya gangguan) dan dimensi *Impact* (tingkat kerugian akademik yang dirasakan mahasiswa), dengan skala *Likert* 1–5. Data yang terkumpul kemudian dianalisis melalui proses manajemen risiko yang mengacu pada standar *ISO 31000:2018* (Setyaningrum et al., 2024). Penilaian risiko TI perlu dilaksanakan secara terstruktur menggunakan kerangka manajemen risiko yang sesuai guna menghasilkan strategi mitigasi yang tepat bagi organisasi(Wijaya & Manuputty, 2022)

Proses Manajemen Risiko

Proses manajemen risiko dalam penelitian ini terdiri atas beberapa tahapan yang berjalan secara sistematis dan berkesinambungan, sebagaimana diuraikan berikut.

Penentuan konteks dalam penelitian ini difokuskan pada fungsionalitas, keamanan operasional, dan keandalan SIAKAD dari sudut pandang mahasiswa sebagai pengguna akhir. Konteks internal meliputi kebiasaan mahasiswa dalam berinteraksi dengan sistem dan tingkat kesadaran keamanan informasi (*security awareness*), sedangkan konteks eksternal mencakup ancaman siber dan lonjakan *traffic* pada masa pengisian KRS.Selanjutnya dilakukan penilaian risiko (*risk assessment*) yang terdiri dari tiga tahap.

Berdasarkan penelitian terdahulu, ancaman umum pada sistem informasi akademik mencakup penyalahgunaan hak akses, kegagalan penginputan data, hingga kegagalan peladen (*server down*) (Sahibu et al., 2024). Selain itu, ancaman seperti akses ilegal (*Brute Force*), rekayasa sosial (*Phishing*), dan kesalahan fungsionalitas sistem juga teridentifikasi sebagai risiko yang berpotensi mengganggu layanan akademik.

Analisis risiko dilakukan dengan pendekatan semi-kuantitatif menggunakan rata-rata skor jawaban kuesioner. Setiap risiko dihitung nilai *Likelihood* dan *Impact*-nya kemudian dikalikan untuk menghasilkan skor risiko. Kriteria *Likelihood* dan *Impact* yang digunakan disajikan pada Tabel 1 dan Tabel 2.

Tabel 1. Kriteria Likelihood

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

(Setyaningrum et al., 2024)

Tabel 2. Kriteria Dampak Risiko

Nilai	Keterangan	Kriteria
1	Sangat Rendah	Kesalahan kecil (misalnya salah input) yang mudah diperbaiki tanpa mempengaruhi operasional. Tidak berdampak pada privasi atau integritas data
2	Rendah	Human error menyebabkan pekerjaan tambahan atau perbaikan manual, namun tidak berdampak pada data sensitif atau akses tidak sah.
3	Sedang	Dampak moderat. Menghambat proses administrasi (seperti delay pengisian KRS) sehingga mahasiswa perlu menunggu beberapa jam agar sistem pulih.
4	Tinggi	Dampak besar. Mengganggu status akademik mahasiswa, seperti data nilai yang salah/hilang, KRS tertunda lama melewati jadwal, atau adanya potensi akun dibajak oleh pihak yang tidak bertanggung jawab.
5	Sangat Tinggi	Human error atau kontrol lemah memungkinkan kebocoran data pribadi/akademik skala besar,penyalahgunaan akses, atau pelanggaran hukum. Risiko reputasi institusi signifikan.

(Setyaningrum et al., 2024)

Evaluasi risiko adalah proses membandingkan antar tingkatan level risiko berdasarkan analisis untuk membantu pengambilan keputusan (Geofanny & Tanaamah, 2022).Hasil perkalian *Likelihood* × *Impact* dipetakan ke dalam matriks risiko dengan tiga kategori, yaitu Rendah (*Low*) untuk skor 1–4, Sedang (*Medium*) untuk skor 5–10, dan Tinggi (*High*) untuk skor di atas 10 (Setyaningrum et al., 2024).

Tahap berikutnya adalah perlakuan risiko (*risk treatment*), di mana strategi pengendalian dipilih berdasarkan level risiko yang telah dievaluasi. Terdapat empat opsi perlakuan risiko yaitu penghindaran (*avoid*), pengurangan (*reduce*), berbagi (*share*), dan penerimaan (*accept*) (Sarjana et al., 2022) . Penerapan ISO 31000 menjadi semakin relevan di era

digital, mengingat banyak organisasi masih menggunakan pendekatan reaktif dalam menangani risiko TI, di mana risiko baru ditangani setelah insiden terjadi (Irsyad & Ilham, 2025).
Sepanjang keseluruhan proses berlangsung, komunikasi dan konsultasi dilakukan melalui penyebaran kuesioner kepada mahasiswa, serta pemantauan dan peninjauan dilakukan untuk memastikan proses manajemen risiko tetap relevan dengan kondisi operasional. Hasil akhir penelitian berupa kesimpulan dan saran yang dapat menjadi rekomendasi bagi pihak fakultas.

HASIL DAN PEMBAHASAN

Hasil Identifikasi dan Analisis Risiko Operasional SIAKAD

Pada tahap ini, dilakukan penyajian hasil identifikasi terhadap risiko-risiko operasional yang terjadi pada Sistem Informasi Akademik (SIAKAD) Universitas XYZ berdasarkan perspektif pengguna akhir (*end-user*). Melalui kuesioner yang disebarkan kepada 23 responden mahasiswa aktif, diperoleh data primer mengenai nilai frekuensi kejadian (*Likelihood*) dan tingkat keparahan (*Impact*) dari lima varian risiko yang teridentifikasi.

Nilai total skor risiko diperoleh dari hasil perkalian antara rata-rata skor *Likelihood* dan *Impact* Skor tersebut kemudian dipetakan ke dalam tiga kategori batas toleransi (*risk appetite*) sesuai dengan kriteria yang telah ditetapkan pada bagian Metode, yaitu Rendah (skor 1–4), Sedang (skor 5–10), dan Tinggi (skor >10). Hasil perhitungan matematis dari seluruh risiko operasional disajikan pada Tabel 3.

Tabel 3. Hasil Perhitungan Skor dan Penentuan Level Risiko Operasional SIAKAD

No	Risiko Operasional Teridentifikasi	Kemungkinan (*L*)	Dampak (*I*)	Skor Risiko	Kategori Level Risiko
1	Bug / Error Fungsionalitas Sistem	3	4	12	Tinggi (High)
2	Akses Ilegal / Brute Force (Pembajakan Akun)	2	5	10	Sedang (Medium)
3	Risiko Ketersediaan / Server Down	2	4	8	Sedang (Medium)
4	Phishing (Penipuan Tautan Login Palsu)	1	5	5	Sedang (Medium)
5	Human Error (Kesalahan Input Data Akademik)	1	5	5	Sedang (Medium)

Hasil analisis menunjukkan bahwa profil risiko operasional SIAKAD di FIKOM Universitas XYZ didominasi oleh tingkat risiko Sedang sebesar 80% (4 risiko) dan tingkat risiko Tinggi sebesar 20% (1 risiko).

Evaluasi Risiko

Tahap evaluasi risiko dilakukan untuk membandingkan hasil skor total analisis risiko dengan batas toleransi risiko (*risk appetite*) yang telah ditetapkan oleh institusi. Proses ini memiliki arti penting untuk menetapkan tingkat urgensi penanganan melalui pemeringkatan prioritas, serta menentukan status akseptabilitas (*risk acceptability*) dari masing-masing risiko operasional SIAKAD. Hasil evaluasi dan prioritasi risiko tersebut disajikan pada Tabel 4.

Tabel 4. Peta Evaluasi, Akseptabilitas, dan Prioritas Risiko SIAKAD

ID	Risiko Operasional SIAKAD	Skor Total	Kategori Level	Peringkat Prioritas
R1	Bug / Error Fungsionalitas Sistem	12	Tinggi (*High*)	1

ID	Risiko Operasional SIAKAD	Skor Total	Kategori Level	Peringkat Prioritas
R2	Akses Ilegal / *Brute Force* (Pembajakan Akun)	10	Sedang (*Medium*)	f
R3	Risiko Ketersediaan / *Server Down*	8	Sedang (*Medium*)	3
R4	*Phishing* (Penipuan Tautan Login Palsu)	5	Sedang (*Medium*)	4
R5	*Human Error* (Kesalahan Input Data)	5	Sedang (*Medium*)	5

Analisis mendalam terhadap status evaluasi risiko dijabarkan sebagai berikut:

1. **Risiko Kategori Tidak Diterima**
   Risiko R1 (*Bug / Error* Fungsionalitas Sistem) merupakan satu-satunya ancaman yang berada pada status tidak diterima karena memiliki skor tertinggi (skor 12). Kondisi ini menandakan bahwa sistem proteksi atau kontrol kualitas internal aplikasi saat ini berada pada kondisi kritis, sehingga membutuhkan intervensi tindakan perbaikan sesegera mungkin guna menghindari kerugian akademik yang lebih luas di sisi pengguna akhir.
2. **Risiko Kategori Diterima dengan Pengawasan**
   Risiko R2, R3, R4, dan R5 diklasifikasikan ke dalam status dapat diterima namun tetap berada dalam pengawasan ketat hingga rutin. Meskipun pihak manajemen Fakultas Ilmu Komputer Universitas XYZ masih mampu menoleransi dampak operasional dari keempat risiko ini dalam aktivitas harian, akumulasi kelalaian tanpa adanya pengawasan berkala berpotensi mengekskalasi skor risiko tersebut ke tingkat yang lebih membahayakan integritas data.

Perlakuan Risiko

Tahap perlakuan risiko merupakan fase merumuskan dan memilih opsi tindakan pengendalian guna mereduksi tingkat risiko operasional SIAKAD Universitas XYZ hingga mencapai batas aman yang dapat ditoleransi (*acceptable risk*). Mengacu pada kerangka ISO 31000:2018, opsi perlakuan yang diterapkan diklasifikasikan ke dalam strategi pengurangan risiko (*mitigate*), pengalihan/berbagi risiko (*share/transfer*), atau penerimaan risiko (*accept*).

Usulan implementasi kontrol penanganan teknis dan administratif untuk kelima risiko operasional dijabarkan secara sistematis pada Tabel 5.

Tabel 5. Perlakuan Risiko SIAKAD

ID	**Kategori Risiko**	**Opsi Perlakuan**	**Usulan Kontrol Kendali teknis / Administratif**
R1	Bug / Error Fungsionalitas Sistem	*Mitigate*	Penerapan User Acceptance Testing (UAT) sebelum pembaruan fitur dirilis dan integrasi modul pelaporan kendala secara langsung.
R2	Akses Ilegal / *Brute Force*	*Mitigate*	Pengaktifan kebijakan enkripsi kredensial login, dan pewajiban reset kata sandi berkala.
R3	Risiko Ketersediaan / *Server Down*	*Share / Transfer*	Penerapan arsitektur pengisian KRS bergelombang dan pengalihan beban trafik menggunakan infrastruktur *cloud hosting* temporal.
R4	*Phishing* (Penipuan Tautan Palsu)	*Mitigate*	Pelaksanaan kampanye edukasi *cyber security awareness* dan standarisasi domain resmi komunikasi fakultas.
R5	*Human Error* (Kesalahan Input Data)	*Mitigate / Accept*	Optimalisasi validasi input data pada sisi klien (*client-side validation*) dan penyediaan layanan *helpdesk* koreksi data

KESIMPULAN

Berdasarkan hasil analisis dan evaluasi manajemen risiko operasional pada Sistem Informasi Akademik (SIAKAD) FIKOM Universitas XYZ menggunakan kerangka kerja ISO 31000:2018, dapat disimpulkan bahwa penilaian berbasis pengalaman pengguna akhir (*end-user*) berhasil memetakan profil risiko secara objektif. Dari lima jenis risiko operasional utama yang diidentifikasi melalui data primer 23 responden mahasiswa, terdapat satu risiko (20%) yang diklasifikasikan ke dalam kategori Tinggi (*High*), yaitu gangguan *Bug* / *Error* Fungsionalitas Sistem dengan skor risiko tertinggi sebesar 12. Risiko ini berada pada status tidak diterima (*unacceptable*) karena dampaknya dapat menghambat proses pengisian rencana studi mahasiswa, sehingga menempatkannya pada prioritas penanganan pertama melalui pengetatan prosedur *User Acceptance Testing* (UAT) sebelum pembaruan fitur dirilis.

Sementara itu, empat risiko operasional lainnya (80%) berada pada kategori Sedang (*Medium*).Risiko-risiko tersebut meliputi ancaman Akses Ilegal/*Brute Force* (skor 10) yang menuntut mitigasi berupa penguatan kebijakan reset kata sandi berkala, risiko ketersediaan peladen/*Server Down* (skor 8) yang direkomendasikan untuk diatasi melalui strategi pengalihan risiko (*risk share/transfer*) memanfaatkan kapasitas *cloud hosting* temporal saat masa beban puncak, serta ancaman *Phishing* (skor 5) dan *Human Error* (skor 5) yang dikendalikan lewat penguatan validasi formulir sistem di sisi klien serta edukasi berkala mengenai keamanan siber (*security awareness*) bagi mahasiswa baru. Penerapan kombinasi strategi kontrol teknis dan administratif ini diharapkan mampu mereduksi tingkat risiko operasional ke dalam batas aman, sekaligus menjamin integritas, kerahasiaan, dan ketersediaan layanan data akademik secara berkelanjutan.

UCAPAN TERIMA KASIH

Ucapan terima kasih setinggi-tingginya penulis sampaikan kepada pengampu mata kuliah, serta rekan-rekan mahasiswa yang telah terlibat dan memberikan dukungan penuh dalam penyelesaian penelitian ini.

DAFTAR PUSTAKA

Ardius, E., Isroqmi, A., Nurdiana, N., Irawan, D., & Hastini, S. (2025). Manajemen Risiko Penggunaan Sistem Informasi Akademik di Universitas ABC Menggunakan ISO 31000. *Jurnal Digital Teknologi Informasi*, *8*(2), 57. https://doi.org/10.32502/digital.v8i2.10428

Geofanny, G. K., & Tanaamah, A. R. (2022). Sistem Manajemen Risiko Berbasis ISO 31000:2018 Di PT. Bawen Mediatama. *Jurnal Teknik Informatika Dan Sistem Informasi* , *9*(4), 2870–2878. http://jurnal.mdp.ac.id

Kurniati, N., Fattah, F., & Hasnawi, M. (2019). Student service performance analysis by using path analysis model. *International Journal of Recent Technology and Engineering*, *8*(2 Special Issue 11), 2580–2582. https://doi.org/10.35940/ijrte.B1308.0982S1119

Lubis, F. S., Praditha, V. S., Lubis, M., Safitra, M. F., & Ramadhan, Y. Z. (2023). IT Risk Analysis Based on Risk Management Using ISO 31000: Case study Registration Application at University XYZ. *Proceedings of the 2023 9th International Conference on Industrial and Business Engineering*, 522–528. https://doi.org/10.1145/3629378.3629464

Marlando, P., Mardiana, & Susanto, M. (2025). Penilaian Risiko Berbasis Iso 31000:2018 Pada Unit Tik Perguruan Tinggi (Studi Kasus: Politeknik Negeri Lampung). *Jurnal Informatika Dan Teknik Elektro Terapan*, *13*(3). https://doi.org/10.23960/jitet.v13i3.6672

Irsyad, M. R. N., & Ilham. (2025). Optimalisasi Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 di Era Digital. *Journal of Information System, Applied, Management, Accounting and Research*, *9*(2), 24–41. https://doi.org/10.52362/jisamar.v9i1.1690

Nadiya, K., Nisa, N. C., Aini, S. A. N., & Jandi, A. U. P. S. (2024). Analisis Manajemen Risiko Pada Sistem Informasi Akademik Menggunakan Framework OCTAVE ALLEGRO. *JORAPI : Journal of Research and Publication Innovation*, *2*(2), 1479–1491. https://jurnal.portalpublikasi.id/index.php/JORAPI/index

Nikmat, A. (2024). Analisis Manajemen Risiko Teknologi Informasi Pada Sistem Informasi Akademik (Siak) Universitas Muhammadiyah Sukabumi (Umm) Menggunakan Iso 31000. *Jurnal Manajemen Dan Teknologi Informasi*, *14*(1), 49–58. https://doi.org/10.59819/jmti.v14i1.3321

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. *Ingenierie Des Systemes d'Information*, *29*(1), 205–218. https://doi.org/10.18280/isi.290121

Sarjana, S., Nardo, R., Hartono, R., & Siregar, Z. H. (2022). *Manajemen Risiko*. Media Sains Indonesia.

Setyaningrum, N. N., Maria, E., Risiko, M., Informasi, S., & Terpadu, S. (2024). *Penerapan iso 31000:2018 untuk manajemen risiko pada sistem informasi sekolah terpadu*. (April), 31–44.

Wijaya, V. P. P., & Manuputty, A. D. (2022). Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *9*(2), 1295–1307. https://doi.org/10.35957/jatisi.v9i2.2087