JURNAL DIGITAL TEKNOLOGI INFORMASI
Vol. 08, No. 02, September 2025, pp. 67-63
E-ISSN 2714-9706 | P-ISSN 2686-4185
Terakreditas Sinta 5 oleh Dirjen Pendidikan Tinggi, Riset, dan Teknologi No. 164/E/KPT/2021

Manajemen risiko penggunaan sistem informasi akademik di universitas abc menggunakan iso 31000

Enggi Ardius [a,1,*]; Asnurul Isroqmi [a,2]; Nita Nurdiana [a,3]; Dendi Irawan [a,4]; Safta Hastini [a,5]
[a] *Universitas PGRI Palembang, Jl. A. Yani 13 Ulu, Palembang, Indonesia*
[1] *enggi.ardius1@univpgri-palembang.ac.id;* [2] *asnurul.isroqmi@univpgri-palembang.ac.id;* [3] *nurdiana78@univpgri-palembang.ac.id;*
[4] *dendiirawan2791@univpgri-palembang.ac.id;* [5] *safta.hastini@univpgri-palembang.ac.id*
** Corresponding author*

Artikel Histori: Diterima 18/06/2025; Revisi 20/08/2025; Terbit 30/09/2025

Abstrak

Universitas ABC sebagai lembaga pendidikan telah menerapkan Teknologi Informasi dan Komunikasi melalui Sistem Informasi Akademik (SISFO) yang terhubung ke jaringan internet untuk mendukung proses bisnis akademik agar lebih cepat dan mudah. Sistem ini menjadi aset penting karena terdiri dari perangkat keras, jaringan komputer, perangkat lunak berupa aplikasi serta basis data, dan pengguna. Pengelolaan dan keamanan informasi SISFO ditangani oleh Divisi IT. SISFO menyediakan layanan seperti kalender akademik, jadwal mengajar, input nilai, pembayaran, KRS, KHS, DKN, dan berbagai kebutuhan akademik lainnya yang terkait pada Dosen dan Mahasiswa. Sistem ini tetap memiliki potensi ancaman yang perlu diantisipasi untuk bertujuan mengetahui kelemahan dan kemungkinan risiko yang akan terjadi. Penelitian ini membahas manajemen risiko teknologi informasi pada SISFO yang berpotensi mengganggu kelancaran proses akademik. Dengan menggunakan metode ISO 31000, penelitian dilakukan melalui tahapan identifikasi, penilaian, dan evaluasi risiko. Hasil menunjukkan bahwa koneksi internet ISP merupakan risiko kritis yang perlu perhatian khusus. Penerapan manajemen risiko yang tepat dapat menjaga keberlangsungan operasional SISFO dan menjadi acuan bagi institusi pendidikan lain dalam pengelolaan sistem informasi akademik.

Kata Kunci: Manajemen Risiko, SISFO, ISO 31000

Pendahuluan

Di era perkembangan saat ini, teknologi memiliki peran penting dalam dunia bisnis sekaligus menjadi penunjang kemajuan universitas maupun organisasi [1]. Pemanfaatan Teknologi Informasi pada perusahaan atau instansi, khususnya universitas, merupakan bagian penting yang tidak terpisahkan dari proses bisnis. Namun, dalam penerapan dan penggunaannya berpotensi menimbulkan berbagai risiko yang dapat mengganggu keberlangsungan bisnis. Oleh karena itu, pengelolaan risiko menjadi aspek yang harus diperhatikan, dan salah satu langkah awal yang dapat dilakukan adalah melakukan pengukuran terhadap risiko teknologi informasi [2]. Risiko adalah suatu kondisi ketidakpastian yang mengandung potensi bahaya atau konsekuensi, baik dari proses yang sedang berlangsung maupun peristiwa yang mungkin terjadi di masa depan. Risiko hadir di seluruh aspek kehidupan, dan pada era milenial dengan revolusi industri 5.0, risiko semakin mudah ditemui serta berpotensi merugikan bisnis perusahaan maupun organisasi [3].

Salah satu sistem yang terintegrasi dengan TIK adalah Sistem Informasi Akademik (SISFO), yang membuat proses bisnis menjadi lebih cepat dan praktis, sehingga seluruh aktivitas di Universitas ABC dapat berjalan optimal. Universitas ABC merupakan perguruan tinggi swasta di Provinsi Sumatera Selatan yang telah menerapkan aktivitas akademik berbasis online, terintegrasi dengan pembelajaran daring melalui e-learning dan SPADA Indonesia sejak 2018. Sistem Informasi Akademik (SISFO) dilengkapi dengan berbagai fasilitas dan fitur yang mendukung interaksi seluruh civitas akademika, termasuk mahasiswa, dosen, pengelola. Melalui SISFO, berbagai kegiatan dapat dilakukan, seperti pengelolaan kalender akademik, pembayaran, jadwal, pendaftaran mahasiswa baru, data dosen dan mahasiswa, biaya kuliah, serta layanan akademik lainnya.

Hingga saat ini, Divisi IT belum sepenuhnya melakukan analisis terhadap penyebab permasalahan aset TI, seperti server yang sering down akibat listrik padam dan suhu ruangan tinggi, rendahnya kesadaran melakukan backup data, kesalahan operasional pengguna SISFO, lemahnya pengawasan

https://doi.org/10.32502/digital.v8i2.10428

P-ISSN : 2686-4185
E-ISSN : 2714-9706

pembaruan aplikasi dan pengelolaan port server, ketiadaan firewall, serta kurangnya kontrol hak akses dan pemantauan bugs maupun error secara berkala. Untuk mengatasinya, diperlukan identifikasi ancaman, analisis kerentanan, penilaian probabilitas dan dampak, serta penerapan kontrol dan pendokumentasian hasil.

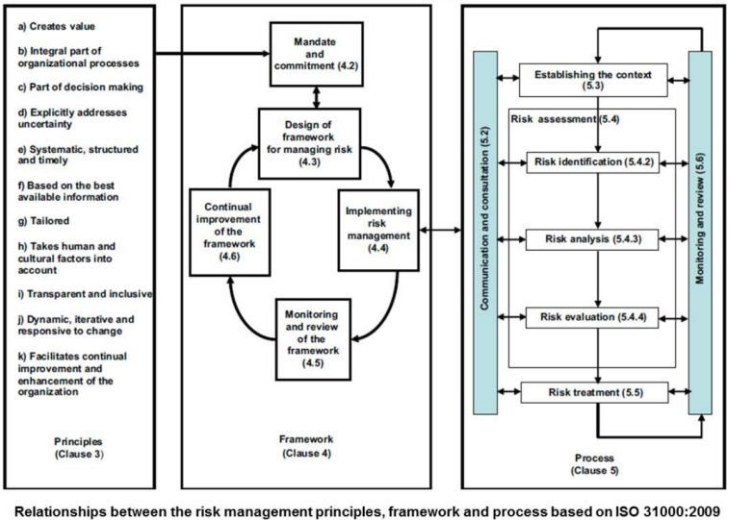
Sistem informasi rentan terhadap berbagai risiko, mulai dari kegagalan akibat bencana alam, kesalahan manusia, kebocoran data oleh peretas, kerusakan sistem karena virus, kebakaran, dan lain sebagainya [4]. Penelitian ini menerapkan metode ISO 31000 yang mencakup proses identifikasi, evaluasi risiko, serta pemeliharaan sistem dan aset pendukung guna memastikan kinerja sistem di masa mendatang [5]. ISO 31000 memberikan kerangka kerja standar internasional yang dapat digunakan dalam mengidentifikasi, menganalisis, mengevaluasi, mengendalikan, dan memantau risiko yang mungkin terjadi [6].

Penelitian ini bertujuan untuk memastikan sistem berjalan secara efektif dan aman dalam mendukung pencapaian tujuan Universitas ABC, sekaligus meminimalkan risiko yang ada maupun yang berpotensi muncul, serta memberikan rekomendasi tepat terkait pengelolaan risiko di masa mendatang.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif untuk menjelaskan dan menganalisis ancaman, kerentanan, dampak, serta aset yang berisiko terhadap sistem dan pendukungnya, dengan menerapkan ISO 31000 sebagai langkah pencegahan dan penanganan keamanan informasi. Untuk memenuhi kebutuhan penelitian, data dikumpulkan melalui tiga metode. Pertama, wawancara dengan narasumber utama seperti Kepala Divisi IT Infokom, Kasubbag Analisis Data Infokom, pengembang aplikasi, dan staf teknisi yang mengelola SISFO Universitas ABC. Kedua, observasi langsung pada aplikasi SISFO dan ruang server Universitas ABC guna mengidentifikasi risiko yang pernah terjadi serta alur proses bisnis. Ketiga, dokumentasi berupa foto kegiatan wawancara, observasi, dan kuesioner yang diisi oleh dosen, karyawan, serta mahasiswa pengguna SISFO [4]. Untuk memastikan manajemen risiko berjalan secara efisien, efektif, dan konsisten, ISO 31000 memberikan panduan kepada organisasi dengan berlandaskan pada tiga pilar utama, yaitu prinsip, kerangka kerja, dan proses [7]. Menurut ISO 31000:2018, manajemen risiko dipahami sebagai serangkaian aktivitas terkoordinasi yang bertujuan untuk mengarahkan dan mengendalikan organisasi dalam menghadapi risiko, di mana risiko dimaknai sebagai konsekuensi dari ketidakpastian terhadap pencapaian tujuan organisasi [8].

Penelitian ini dilakukan di Universitas ABC. Waktu penelitian dilaksanakan bulan Juli sampai dengan bulan September 2025. Manajemen risiko merupakan proses identifikasi, analisis, dan evaluasi risiko yang bertujuan menghasilkan rekomendasi untuk pengelolaannya.



Gambar 1. Kerangka Kerja ISO 31000 dan Tahapan Manajemen Risiko

Pada gambar 1 diatas menjelaskan kerangka kerja ISO 31000 yang terdiri dari 5 tahapan. Tahap pertama adanya mandat dan komitmen dari pimpinan universitas. Dukungan penuh dari pihak manajemen menjadi kunci agar pengelolaan risiko dapat berjalan efektif dan terarah. Tahap kedua ilakukan desain kerangka kerja yang mencakup penetapan struktur organisasi, pembagian peran dan tanggung jawab, serta penyediaan sumber daya yang dibutuhkan untuk mendukung pengelolaan risiko. Tahap ketiga adalah implementasi, yaitu penerapan manajemen risiko secara langsung dalam operasional SISFO. Hal ini mencakup kegiatan seperti pemantauan server, pengamanan data, serta pengaturan akses pengguna

agar sistem tetap berjalan optimal dan aman. Tahap keempat dilakukan monitoring dan review untuk meninjau secara berkala efektivitas dari strategi manajemen risiko yang telah diterapkan, sehingga dapat diketahui apakah masih relevan atau perlu disesuaikan serta tahap kelima diiringi dengan perbaikan berkelanjutan, yakni evaluasi serta peningkatan pengelolaan risiko sesuai perkembangan kebutuhan universitas dan kemajuan teknologi. Dengan demikian, sistem informasi akademik dapat tetap andal, aman, dan mendukung seluruh aktivitas akademik universitas secara optimal. Tahapan manajemen risiko secara universal yang terdiri dari dua tahapan utama. Tahap pertama adalah risk assessment, yang mencakup tiga proses: identifikasi risiko untuk mengenali potensi risiko dalam setiap proses bisnis organisasi, analisis risiko sebagai kajian untuk memastikan keberhasilan proyek sesuai tujuan, serta evaluasi risiko. Tahap kedua adalah risk treatment, yakni pemberian rekomendasi atau tindakan untuk menangani dan meminimalkan risiko yang mungkin terjadi, khususnya pada aplikasi SISFO.

Hasil dan Pembahasan

a. Penilaian Risiko (Risk Assessment)

Pada tahap ini, peneliti melakukan penilaian risiko terhadap penggunaan SISFO berdasarkan pedoman analisis manajemen risiko ISO 31000, yang mencakup tiga proses utama, yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko.

1. Identifikasi Risiko

Identifikasi kerentanan aset dilakukan untuk mengenali potensi ancaman terhadap sistem informasi, dengan data jenis dan nilai aset diperoleh melalui wawancara serta observasi.

Tabel 1. Identifikasi Daftar Aset SISFO

Kategori Aset TI	Nama Aset SISFO
Data	Data Mata Kuliah
	Data Pembayaran
	Data Nilai
	Data User
Perangkat Lunak (Software)	Aplikasi SISFO
Perangkat Keras (Hardware)	Server
	Monitor
	Mikrotik
	Modem Internet
Sumber Daya Manusia (Brainware)	Pengelola SISFO
	Pengguna SISFO
Sarana Pendukung	Genset
	UPS
	AC

Setelah mengidentifikasi aset yang berkaitan dengan SISFO, meliputi data, perangkat keras, perangkat lunak, sumber daya manusia, dan sarana pendukung, langkah berikutnya adalah mengidentifikasi potensi risiko yang mungkin muncul. Peneliti kemudian mengelompokkan risiko tersebut ke dalam tiga faktor, yaitu alam/lingkungan, manusia, serta sistem dan infrastruktur, dengan memberikan nomor ID pada setiap risiko yang ditemukan.

Tabel 2. Identifikasi Kemungkinan Risiko

Faktor	Kode Risiko	Kemungkinan
Alam atau Linkungan	R001	Banjir
	R002	Kebakaran
	R003	Gempa Bumi
Manusia	R004	Penyalahgunaan Hak Akses
	R005	Human Error
	R006	Adware, malware, spyware
	R007	Pencuruan/Spam
Sistem atau Infrastruktur	R008	Kerusakan Server
	R009	Kerusakan Genset
	R010	Server Down
	R011	Gangguan Koneksi Internet
	R012	Data Corrupt
	R013	Gangguan Web/Database Server

P-ISSN : 2686-4185
E-ISSN : 2714-9706

Selanjutnya, terhadap risiko-risiko yang telah teridentifikasi pada tabel 2, dilakukan analisis untuk menentukan dampak-dampak yang mungkin timbul.

Tabel 3. Identifikasi Dampak Risiko

Kode Risiko	Kemungkinan	Dampak
R001	Banjir	Kegiatan/aktifitas Universitas jadi terhenti
R002	Kebakaran	Kegiatan/aktifitas Universitas jadi terhenti
R003	Gempa Bumi	Infrastruktur rusak dan aktivitas terhenti
R004	Penyalahgunaan Hak Akses	Data user akan disalahgunakan
R005	Human Error	Proses aktifitas universitas terganggu
R006	Adware, malware, spyware	Server dan Aplikasi akan terhenti
R007	Pencuruan/Spam	Data SISFO akan hilang
R008	Kerusakan Server	User tidak bisa mengakses aplikasi
R009	Kerusakan Genset	Aktifitas universitas akan terganggu
R010	Server Down	Aktifitas kegiatan universitas terganggu
R011	Gangguan Koneksi Internet	Terganggu untuk mengakases aplikasi
R012	Data Corrupt	Data bisa hilang dan aktifitas universitas terganggu
R013	Gangguan Web/Database Server	Kegiatan aktifitas universitas terganggu

2. Analisis Risiko

Analisis risiko dilakukan setelah identifikasi risiko dan dampaknya, dengan menggunakan dua kriteria utama, yaitu likelihood dan impact, yang mengukur frekuensi serta tingkat dampak kemungkinan terjadinya risiko.

Tabel 4. Identifikasi Dampak Risiko

Kode Risiko	Kemungkinan	Likelihood	Impact
R001	Banjir	1	5
R002	Kebakaran	1	5
R003	Gempa Bumi	1	5
R004	Penyalahgunaan Hak Akses	2	2
R005	Human Error	5	1
R006	Adware, malware, spyware	3	3
R007	Pencuruan/Spam	2	3
R008	Kerusakan Server	1	5
R009	Kerusakan Genset	3	3
R010	Server Down	4	3
R011	Gangguan Koneksi Internet	5	4
R012	Data Corrupt	1	3
R013	Gangguan Web/Database Server	2	4

3. Evaluasi Risiko

Tahap akhir dari risk assessment adalah evaluasi risiko dengan menggunakan matriks risiko yang membagi risiko ke dalam tiga tingkat, yaitu rendah, sedang, dan tinggi. Nilai likelihood dan impact yang telah ditentukan pada tahap sebelumnya kemudian dipetakan sesuai kategori dalam matriks tersebut. Pada tabel. 7 dibawah ini merupakan tabel matrix evaluasi resiko yang sudah di tentukan risk level berdasarkan likelihood dan impact nya.

Tabel 5. Matrix Evaluasi Resiko

Likelihood							
	Certain/Pasti terjadi	5	Medium	Medium	High	High	High
	Likely/Sering	4	Medium	Medium	Medium	High	High
	Possible/Kadang	3	Low	Medium	Medium	Medium	High
	Unlikely/Jarang	2	Low	Low	Medium	Medium	Medium
	Rare/Hampir tidak pernah	1	Low	Low	Low	Medium	Medium
	Impact		1 Insignificant/ Sangat Kecil	2 Minor/ Kecil	3 Moderate/ Biasa	4 Major/ Besar	5 Catastrophic/ Sangat Besar

Tabel 6 berikut menyajikan hasil kemungkinan risiko yang telah dimasukkan ke dalam matriks evaluasi berdasarkan kriteria likelihood dan impact yang ditetapkan pada tahap sebelumnya.

Tabel 6. Matrix Evaluasi Resiko Berdasarkan nilai likelihood dan impact

Likelihood			Impact 1 Insignificant/ Sangat Kecil	2 Minor/ Kecil	3 Moderate/ Biasa	4 Major/ Besar	5 Catastrophic/ Sangat Besar
	Certain/Pasti terjadi	5	R005			R011	
	Likely/Sering	4			R010		
	Possible/Kadang	3			R006 R009		
	Unlikely/Jarang	2		R004	R007	R013	
	Rare/Hampir tidak pernah	1			R012		R001 R002 R003 R008

Setelah seluruh risiko yang teridentifikasi dimasukkan ke dalam matriks evaluasi sesuai nilai likelihood dan impact, risiko-risiko tersebut kemudian dikelompokkan ke dalam tiga tingkat, yaitu tinggi, sedang, dan rendah, berdasarkan 13 kemungkinan risiko yang tercantum pada tabel 6.

Tabel 7. Pengelompokkan Risiko Berdasarkan Tingkatan

Kode Risiko	Kemungkinan	Likelihood	Impact	Level Risiko
R011	Gangguan Koneksi Internet	5	4	High
R010	Server Down	4	3	Medium
R006	Adware, malware, spyware	3	3	Medium
R005	Human Error	5	1	Medium
R007	Pencuruan/Spam	2	3	Medium
R013	Gangguan Web/Database Server	2	4	Medium
R001	Banjir	1	5	Medium
R002	Kebakaran	1	5	Medium
R003	Gempa Bumi	1	5	Medium
R008	Kerusakan Server	1	5	Medium
R009	Kerusakan Genset	3	3	Medium
R004	Penyalahgunaan Hak Akses	2	2	Low
R012	Data Corrupt	1	3	Low

Pada hasil tabel 7, terdapat 1 risiko dengan level high yaitu: R011 (Gangguan Koneksi Internet). Lalu terdapat 9 risiko dengan level medium yaitu: R010, R006, R005, R007, R013, R001, R002, R003 dan R008. Dan terakhir terdapat 2 risiko dengan level low yaitu: R004 dan R0012. Pada hasil penelitian yang lain yang dilakukan oleh Irma Rahayu dkk (2025) yang berjudul Manajemen Risiko Keamanan Aset Teknologi Informasi di DISKOMINFOSANDITIK Kabupaten Sumedang Menggunakan ISO 31000:2018, penelitian ini menemukan 14 potensi risiko, terdiri dari 7 risiko rendah, 3 risiko menengah, dan 4 risiko tinggi. Risiko kategori tinggi, khususnya gangguan koneksi internet, menjadi prioritas penanganan melalui evaluasi ISP dan jaringan di Dinas Komunikasi dan Informatika Persandian dan Statistik Kabupaten Sumedang [9].

4. Perlakuan Risiko

Setelah proses analisis risiko, tahap selanjutnya adalah Risk Treatment atau perlakuan risiko, yakni pemberian usulan tindakan terhadap risiko yang telah dikelompokkan berdasarkan tingkat risiko pada tabel 7.

Tabel 8. Usulan Perlakuan Pada Risiko

Kode Risiko	Kemungkinan	Level Risiko	Usulan Tindakan Risiko
R011	Gangguan Koneksi Internet	High	Laporkan pada teknisi ISP bahakn jika perlu ganti ISP yang baru
R010	Server Down	Medium	Melakukan perbaikan dan pengecekan terhadap server dan database
R006	Adware, malware, spyware	Medium	Melakukan scanning dan backup database secara berkala

P-ISSN : 2686-4185
E-ISSN : 2714-9706

R005	Human Error	Medium	Melakukan pelatihan atau sosialisasi rutin terhadap pengguna
R007	Pencuruan/Spam	Medium	Menambahkan firewall dan backup berkala
R013	Gangguan Web/Database Server	Medium	Melakukan perbaikan dan pengecekan terhadap service dan database
R001	Banjir	Medium	Menyediakan tempat yang aman terhadap banjir (backup)
R002	Kebakaran	Medium	Menyiapkan alat pemadam kebakaran
R003	Gempa Bumi	Medium	Menyediakan server cadangan dilokasi aman
R008	Kerusakan Server	Medium	Melakukan pengecekan dan perbaikan berkala pada server
R009	Kerusakan Genset	Medium	Melakukan pengecekan berkala pada genset, beli UPS yang memiliki daya tampung waat tinggi
R004	Penyalahgunaan Hak Akses	Low	Melakukan perbaikan pada aplikasi/sistem berkala
R012	Data Corrupt	Low	Melakukan backup secara berkala

Pada hasil tabel 8, terdapat kemungkinan risiko dengan level high (tinggi) yaitu gangguan koneksi internet Gangguan koneksi internet sebagai risiko dengan level tinggi pada aplikasi SISFO dapat terjadi akibat kualitas layanan ISP yang tidak stabil, keterbatasan bandwidth, maupun infrastruktur jaringan internal yang kurang optimal. Jika tidak ditangani, hal ini berpotensi menghambat proses akademik seperti registrasi, akses nilai, dan administrasi. Untuk mengatasinya, Universitas ABC perlu melakukan evaluasi layanan ISP, menyiapkan koneksi cadangan, memperkuat infrastruktur jaringan, serta menerapkan monitoring dan pemeliharaan rutin agar koneksi tetap stabil dan layanan SISFO berjalan optimal.

Studi kasus di Universitas ABC memberikan kontribusi signifikan dalam memperluas pemahaman mengenai implementasi manajemen risiko teknologi informasi berbasis ISO 31000 di lingkungan pendidikan tinggi. Penelitian ini menyoroti risiko kritis berupa gangguan koneksi internet sebagai faktor dominan yang berpotensi menghambat kelancaran proses akademik, sekaligus menunjukkan bahwa pendekatan sistematis melalui tahapan identifikasi, analisis, evaluasi, serta perlakuan risiko mampu memberikan gambaran yang jelas mengenai prioritas penanganan. Dengan demikian, hasil penelitian ini tidak hanya relevan bagi Universitas ABC, tetapi juga dapat dijadikan model rujukan bagi institusi pendidikan lain dalam mengembangkan strategi pengelolaan risiko teknologi informasi yang adaptif, berkesinambungan, dan selaras dengan dinamika perkembangan teknologi.

Simpulan

Berdasarkan hasil penelitian, analisis risiko teknologi informasi pada SISFO dengan menggunakan ISO 31000 dilakukan melalui beberapa tahapan, mulai dari komunikasi dan konsultasi, penentuan konteks, penilaian risiko, analisis risiko, evaluasi risiko, perlakuan risiko, hingga monitoring dan review.

Dari hasil analisis risiko ditemukan 1 kemungkinan risiko dengan level High yaitu gangguan koneksi internet. Kemudian terdapat 10 kemungkinan risiko dengan level medium yaitu server down, adware, malware, spyware, human error, pencuruan/spam, gangguan web/database server, banjir, kebakaran, gempa bumi, kerusakan server dan kerusakan genset. Terakhir terdapat 2 kemungkinan risiko dengan level low yaitu penyalahgunaan hak akses, data corrupt.

Dengan adanya penelitian ini, diharapkan hasilnya dapat menjadi pedoman bagi Universitas dalam meminimalkan potensi risiko yang mungkin timbul, melalui penerapan perlakuan risiko pada tabel 8. Khususnya untuk gangguan koneksi internet, upaya yang dilakukan adalah mengganti ISP terbaru serta melaporkannya kepada teknisi ISP agar proses bisnis universitas tetap berjalan dengan baik.

Daftar Pustaka

[1] W. Harefa and K. D. Hartomo, “Risk Management Analysis Using the ISO 31000 Framework in Warehouse Information Systems,” J. Informatics Eng. Inf. Syst., vol. 9, no. 1, 2022.
[2] M. Miftakhatun, “Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000,” J. Comput. Sci. Eng., vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.
[3] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, “Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ,” JURIKOM (Jurnal Ris. Komputer), vol. 7, no. 1, p. 91, 2020, doi: 10.30865/jurikom.v7i1.1791.
[4] I. Setiawan, A. R. Sekarini, R. Waluyo, and F. N. Afiana, “Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto,” MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput., vol. 20, no. 2, pp. 389–396, 2021, doi: 10.30812/matrik.v20i2.1093.

[5] R. I. Liperda and U. Ayu Septia Nieng, “Analisis Manajemen Resiko Aplikasi Mypertamina Dengan Menggunakan Iso 31000,” INFOTECH J., vol. 9, no. 2, pp. 361–370, 2023, doi: 10.31949/infotech.v9i2.6232.
[6] R. H. Pangestu, A. D. Cahyono, and P. F. Tanaem, “Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Mengunakan ISO 31000,” J. Comput. Inf. Syst. Ampera, vol. 2, no. 1, pp. 43–57, 2021, doi: 10.51519/journalcisa.v2i1.59.
[7] G. H. S. Rampini, H. Takia, and F. T. Berssaneti, “Critical success factors of risk management with the advent of ISO 31000 2018 - Descriptive and content analyzes,” Procedia Manuf., vol. 39, pp. 894–903, 2019, doi: 10.1016/j.promfg.2020.01.400.
[8] T. Parviainen, F. Goerlandt, I. Helle, P. Haapasaari, and S. Kuikka, “Implementing Bayesian networks for ISO 31000:2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and future research directions,” J. Environ. Manage., vol. 278, no. March 2020, 2021, doi: 10.1016/j.jenvman.2020.111520.
[9] Irma Rahayu, David Setiadi, and Dwi Yuniarto, “Manajemen Risiko Keamanan Aset Teknologi Informasi di DISKOMINFOSANDITIK Kabupaten Sumedang Menggunakan ISO 31000:2018,” J. Tek. Mesin, Ind. Elektro dan Inform., vol. 4, no. 1, pp. 255–264, 2025, doi: 10.55606/jtmei.v4i1.4819.