Scripta Economica:
Journal of Economics, Management, and Accounting
Vol 1 No 1 Juli 2025, Hal 67-77
ISSN: 3110-0848 (Print) ISSN: 3109-970X (Electronic)
Open Access: https://scriptaintelektual.com/scripta-economica

Risiko Operasional dalam Teknologi Informasi: Kajian Literatur Mengenai Mekanisme Identifikasi, Penilaian, dan Dampaknya terhadap Manajemen Risiko

Adelia Nafisah Balqis[1*], Salma Nabila Ramadhani[2], Alvianus Kristian Sumual[3]
[1-3] Institut Teknologi Kalimantan, Indonesia
email: 17221021@student.itk.ac.id[1], 17221004@student.itk.ac.id[2], alvianus.sumual@lecturer.itk.ac.id[3]

Article Info :
Received:
20-6-2025
Revised:
29-6-2025
Accepted:
22-7-2025

Abstract

This study presents a systematic literature review on operational risk in information technology, focusing on mechanisms for identifying risks, approaches for assessing them, and their implications for broader risk management practices. The findings show that the identification of IT operational risks requires structured procedures that incorporate business process analysis, technology audits, anomaly detection, and evaluations of human factors to reveal potential vulnerabilities that may disrupt organizational operations. Frameworks such as ISO 31000 and COBIT are widely used to guide institutions in identifying, categorizing, and managing technology-related risks in a consistent and comprehensive manner. Emerging methods that utilize artificial intelligence, big data analytics, and predictive modeling have also contributed to improving the accuracy of risk detection in increasingly complex digital environments.The review further demonstrates that IT operational risks have substantial impacts on organizational resilience, financial performance, service continuity, and regulatory compliance. Technological failures can hinder decision-making processes, damage user trust, and weaken long-term institutional stability. Therefore, integrating IT operational risk management into enterprise-wide strategies is essential to ensure operational reliability and preparedness in the digital era.
.

Keywords: *Operational risk, information technology, risk identification, risk assessment, risk management.*

Akbstrak

Studi ini menyajikan tinjauan sistematis literatur tentang risiko operasional dalam teknologi informasi, dengan fokus pada mekanisme identifikasi risiko, pendekatan untuk mengevaluasinya, dan implikasinya bagi praktik manajemen risiko yang lebih luas. Temuan menunjukkan bahwa identifikasi risiko operasional TI memerlukan prosedur terstruktur yang mencakup analisis proses bisnis, audit teknologi, deteksi anomali, dan evaluasi faktor manusia untuk mengidentifikasi potensi kerentanan yang dapat mengganggu operasional organisasi. Kerangka kerja seperti ISO 31000 dan COBIT secara luas digunakan untuk membimbing institusi dalam mengidentifikasi, mengkategorikan, dan mengelola risiko terkait teknologi secara konsisten dan komprehensif. Metode baru yang memanfaatkan kecerdasan buatan, analisis big data, dan pemodelan prediktif juga telah berkontribusi dalam meningkatkan akurasi deteksi risiko di lingkungan digital yang semakin kompleks. Tinjauan ini juga menunjukkan bahwa risiko operasional TI memiliki dampak signifikan terhadap ketahanan organisasi, kinerja keuangan, kelangsungan layanan, dan kepatuhan regulasi. Gagal teknologi dapat menghambat proses pengambilan keputusan, merusak kepercayaan pengguna, dan melemahkan stabilitas institusional jangka panjang. Oleh karena itu, mengintegrasikan manajemen risiko operasional TI ke dalam strategi perusahaan secara keseluruhan sangat penting untuk memastikan keandalan operasional dan kesiapan di era digital.

Kata Kunci: Risiko operasional, teknologi informasi, identifikasi risiko, penilaian risiko, manajemen risiko.

PENDAHULUAN

Perkembangan pesat teknologi informasi (TI) telah membawa manfaat besar bagi organisasi dalam hal efisiensi operasional dan transformasi bisnis. Namun, di balik potensi tersebut, risiko operasional TI menjadi semakin kompleks dan menantang bagi manajemen risiko perusahaan. Dalam literatur terkini, banyak peneliti menyoroti bahwa identifikasi dan mitigasi risiko operasional TI tidak dapat diabaikan karena gangguan teknologi dapat menimbulkan kerugian finansial maupun reputasi.

Studi-studi seperti yang dilakukan oleh Asmarawati & Dewi (2024) menegaskan perlunya kerangka manajemen yang sistematis agar Risiko Operasional TI dapat diukur dan dikendalikan.

Salah satu tantangan utama dalam mengelola risiko operasional TI adalah kurangnya kesadaran di tingkat manajerial terhadap eksposur siber. Menurut survei PwC Global Risk Survey 2023, sekitar 37% organisasi menganggap mereka sangat terekspos terhadap risiko siber, sedangkan 39% menilai risiko inflasi lebih tinggi. Angka tersebut menunjukkan bahwa risiko TI bukanlah isu teknis semata, melainkan bagian penting dari profil risiko strategis perusahaan. Komponen ini menjadi motivasi bagi banyak perusahaan untuk merevisi kebijakan manajemen risiko mereka, terutama dalam integrasi risiko operasional TI ke dalam kerangka ISO 31000 atau kerangka lain yang komprehensif.

Literatur manajemen risiko TI menekankan pentingnya kerangka formal seperti ISO 31000 dan COBIT untuk mendeteksi potensi ancaman operasional. Sebagai contoh, Thenu, Wijaya, & Rudianto (2020) dalam studinya pada perusahaan teknologi menunjukkan bahwa COBIT 5 dapat digunakan sebagai alat identifikasi dan kontrol risiko TI dengan efektif. Demikian pula, Ahkmad (2024) menerapkan ISO 31000 dalam optimalisasi proyek TI untuk mengidentifikasi area rawan kegagalan sistem, kesalahan manusia, dan gangguan teknologi lainnya. Pendekatan ini memperkuat pemahaman bahwa identifikasi risiko operasional TI harus dilakukan secara sistematis dan berkelanjutan.

Penilaian risiko operasional TI juga menjadi aspek krusial dalam literatur manajemen risiko. Penelitian Asmarawati & Dewi (2024) mengadopsi ISO 31000 untuk menilai risiko operasional dan risiko keuangan pada perusahaan, menunjukkan bahwa metrik seperti probabilitas kegagalan sistem dan dampak finansial dapat diukur dengan metode kuantitatif dan kualitatif. Studi Fuji, Supriadi, & Junaedi (2025) menyajikan strategi manajemen risiko berbasis literatur, yang mencakup penilaian secara berlapis (multilevel) untuk menangani ancaman dari sisi data, infrastruktur, dan sumber daya manusia. Pendekatan ini penting agar manajemen tidak hanya bereaksi terhadap insiden, tetapi melakukan mitigasi proaktif berdasarkan hasil penilaian risiko yang komprehensif.

Adapun dampak risiko operasional TI terhadap organisasi juga dibahas secara luas dalam kajian literatur, terutama di sektor keuangan dan pemerintahan. Misalnya, Sutigar, Bhisma, Firmansyah, & Wulansari (2024) melakukan review literatur di instansi pemerintahan dan menemukan bahwa serangan siber dan kegagalan sistem TI dapat mengganggu pelayanan publik serta menurunkan kepercayaan masyarakat. Di sektor keuangan, Capriani & Dana (2016) menunjukkan bahwa risiko operasional dapat menekan profitabilitas BPR melalui gangguan sistem dan kerugian non-transaksional. Temuan ini mempertegas bahwa dampak operasional TI tidak hanya bersifat teknis, tetapi juga memiliki implikasi strategis dan finansial yang signifikan.

Untuk memperkuat argumen mengenai urgensi pengelolaan risiko operasional TI, berikut data survei terkini yang merefleksikan eksposur risikonya di organisasi global:

Tabel 1. Paparan Risiko Operasional TI di Organisasi Global

Aspek Risiko	Persentase Organisasi
Organisasi yang merasa sangat terekspos terhadap risiko siber	37 %
Organisasi yang mengalami pelanggaran data dengan biaya US$ 1–20 juta dalam 3 tahun terakhir	27 %
Perusahaan global yang melaporkan insiden keamanan terkait AI dalam 12 bulan terakhir	86 %

Sumber: *PwC Global Risk Survey 2023, PwC Global Digital Trust Insights 2023, Cisco Cybersecurity Readiness Index 2025*

Data di atas memperjelas bahwa risiko operasional TI bukanlah potensi kecil; banyak organisasi melaporkan paparan yang signifikan, baik dari sisi siber maupun insiden teknologi baru seperti AI. Literatur juga menunjukkan bahwa teknologi itu sendiri dapat menjadi sumber mitigasi sekaligus ancaman. Contohnya, Capriani & Dana (2016) menyoroti bahwa meskipun TI meningkatkan efisiensi, risiko operasional muncul dari kesalahan sistem, bug, dan kegagalan integrasi. Sementara itu, Caseba & Dewayanto (2024) dalam kajian sistematik mereka menyoroti bahwa adopsi AI, big data, dan blockchain dalam fintech payment meningkatkan risiko penipuan komputer (*computer fraud*), yang

memerlukan mekanisme identifikasi dan kontrol khusus. Hal ini menandai dualitas teknologi: sebagai enabler dan sekaligus risiko operasional yang harus diatur dengan hati-hati.

Konsep manajemen risiko TI dalam literatur juga berkembang ke arah integrasi dengan manajemen risiko korporasi yang lebih luas. Penelitian Budianto (2023) misalnya, melakukan pemetaan bibliometrik risiko operasional dalam industri keuangan syariah dan konvensional, dan menemukan bahwa risiko TI harus dilihat dalam konteks struktur risiko perusahaan secara keseluruhan. Begitu pula dengan Mardikaningsih, Halizah, Nuraini, Darmawan, & Hardyansah (2024), yang menelaah manajemen risiko rantai pasokan global dan menyoroti bahwa gangguan TI di rantai pasokan dapat memicu risiko operasional skala besar. Perspektif ini memperkuat bahwa manajemen risiko TI tidak bisa dilepaskan dari manajemen risiko strategis dan operasional perusahaan secara menyeluruh.

Kajian literatur mengenai risiko operasional TI menekankan perlunya mekanisme mitigasi dinamis dan adaptif. Strategi seperti kerangka ISO 31000, penggunaan COBIT, audit berkala, simulasi insiden, dan pengujian pemulihan sistem menjadi sangat penting dalam menjaga ketahanan organisasi. Studi Fuji et al. (2025) menekankan bahwa literatur modern menyoroti strategi multilevel dan integratif, yang menggabungkan identifikasi, penilaian, serta monitoring risiko TI secara berkesinambungan. Dengan demikian, manajemen risiko operasional TI harus diadopsi sebagai bagian integral dari governance perusahaan, agar organisasi dapat menghadapi tantangan teknologi dengan percaya diri dan proaktif.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kajian literatur sistematis yang disusun melalui tahapan identifikasi, seleksi, evaluasi, dan sintesis terhadap publikasi ilmiah yang relevan dengan risiko operasional dalam teknologi informasi. Proses pencarian sumber dilakukan pada basis data akademik seperti Google Scholar, DOAJ, SINTA, dan portal jurnal universitas. Kriteria inklusi mencakup artikel yang dipublikasikan antara tahun 2016 hingga 2025, memiliki fokus pada risiko operasional TI, dan menerapkan pendekatan analitis maupun deskriptif dalam pembahasannya. Tahapan ini memastikan bahwa literatur yang dianalisis memiliki relevansi tinggi terhadap topik penelitian dan mencerminkan perkembangan terbaru dalam praktik manajemen risiko TI.

Setelah proses seleksi dilakukan, setiap artikel dianalisis menggunakan teknik content analysis untuk mengidentifikasi tema utama berupa mekanisme identifikasi risiko, penilaian risiko, serta dampaknya terhadap manajemen risiko organisasi. Proses analisis dilakukan dengan mengelompokkan temuan-temuan penting dari masing-masing studi ke dalam kategori tematik untuk kemudian dibandingkan guna menemukan pola atau kecenderungan yang konsisten. Sintesis dilakukan secara naratif, sehingga dapat menggambarkan hubungan antara konsep, metode, dan hasil temuan terkait pengelolaan risiko operasional TI. Pendekatan metodologis ini memberikan gambaran komprehensif yang diperlukan untuk menarik kesimpulan berbasis literatur mengenai efektivitas berbagai strategi manajemen risiko operasional TI.

HASIL DAN PEMBAHASAN

Mekanisme Identifikasi Risiko Operasional TI

Pemahaman mendalam terhadap mekanisme identifikasi risiko operasional TI menjadi fondasi utama dalam memastikan stabilitas sistem dan keberlanjutan proses bisnis, terutama ketika organisasi semakin bergantung pada teknologi digital di seluruh lini operasional perusahaan. Kajian literatur menunjukkan bahwa pemetaan risiko secara sistematis menuntut organisasi untuk menelaah titik-titik kerentanan yang dapat muncul dari kegagalan perangkat keras, kesalahan perangkat lunak, hingga gangguan jaringan yang berulang. Penelitian Asmarawati dan Dewi (2024) menggarisbawahi bahwa kerangka ISO 31000 memungkinkan proses identifikasi dilakukan secara terstruktur melalui pengenalan sumber risiko, peristiwa pemicu, dan konsekuensi potensial. Banyak organisasi yang menempatkan aktivitas identifikasi sebagai langkah awal paling kritis karena proses tersebut mempengaruhi kualitas penilaian risiko dan efektivitas mitigasi pada tahap berikutnya.

Prosedur identifikasi risiko operasional TI menuntut pendekatan metodologis yang menyeluruh, mencakup analisis proses bisnis, audit teknologi, hingga observasi pola insiden historis untuk menemukan celah yang dapat menimbulkan gangguan operasional. Penelitian Ricky (2017) mengemukakan bahwa dalam sektor perbankan, identifikasi risiko harus mempertimbangkan aspek pemilihan perangkat keras dan perangkat lunak yang memiliki konsekuensi langsung terhadap

kontinuitas layanan. Kajian Parera et al. (2022) menemukan bahwa area penyimpanan data yang kurang mendapatkan pengawasan dapat memunculkan risiko seperti kehilangan dokumen digital atau kerusakan integritas data yang berdampak pada proses operasional. Kebutuhan terhadap standar identifikasi yang cermat menjadi semakin menonjol ketika sistem TI semakin kompleks dan saling terhubung.

Penerapan kerangka COBIT 5 sebagai acuan identifikasi risiko operasional TI banyak dibahas dalam literatur karena kerangka tersebut mampu menguraikan proses-proses teknologi secara terperinci sehingga memudahkan pemetaan risiko yang relevan. Studi Thenu, Wijaya, dan Rudianto (2020) menunjukkan bahwa COBIT 5 menyediakan indikator kendali yang dapat memandu organisasi untuk menemukan area risiko berdasarkan domain proses yang spesifik. Penelitian Nisa', Febrianti, dan Ajrina (2023) juga menegaskan bahwa COBIT sangat membantu dalam mengidentifikasi risiko TI di sektor jasa yang memiliki karakteristik operasional dinamis. Ketika organisasi menerapkan kerangka standar, konsistensi identifikasi risiko dapat terjaga dan memperkuat kualitas analisis operasional secara keseluruhan.

Kajian mengenai adopsi teknologi baru seperti AI, big data, dan blockchain menunjukkan bahwa mekanisme identifikasi risiko harus diperluas agar mencakup ancaman berbasis teknologi yang muncul dari integrasi digital yang semakin mendalam. Caseba dan Dewayanto (2024) menemukan bahwa inovasi fintech payment menghadirkan risiko penipuan komputer yang memerlukan teknik identifikasi berbasis deteksi anomali. Penelitian Santorry (2024) juga menekankan bahwa inovasi teknologi finansial memperbesar kebutuhan organisasi untuk memperkuat unit pengawasan risiko karena ancaman operasional dapat bermula dari kesalahan prediksi algoritma maupun gangguan otomatisasi. Identifikasi risiko pada ekosistem digital modern membutuhkan penggabungan antara pendekatan kontrol tradisional dan pemantauan teknologi berkelanjutan.

Tabel 1. Hasil Temuan dari Berbagai Literatur

No	Penulis & Tahun	Fokus Studi	Relevansi Terhadap Identifikasi Risiko TI
1	Asmarawati & Dewi (2024)	ISO 31000 dan risiko operasional	Identifikasi sumber dan pemicu risiko
2	Capriani & Dana (2016)	Risiko operasional perbankan	Identifikasi risiko sistem dan proses
3	Caseba & Dewayanto (2024)	AI, Big Data, Blockchain	Identifikasi risiko penipuan komputer
4	Fuji et al. (2025)	Strategi manajemen risiko TI	Identifikasi melalui audit dan evaluasi
5	Nisa' et al. (2023)	COBIT pada industri jasa	Identifikasi berdasar domain kontrol
6	Thenu et al. (2020)	Risiko TI perusahaan teknologi	Identifikasi celah proses digital
7	Yasirandi et al. (2021)	Risiko operasional layanan informasi	Identifikasi kesalahan operasional manusia
8	Hasibuan (2024)	Risiko operasional bank syariah	Identifikasi prosedur dan proses kerja
9	Parera et al. (2022)	Risiko rekam medis	Identifikasi kelemahan penyimpanan data
10	Ricky (2017)	Risiko perangkat keras dan lunak	Identifikasi kerentanan sistem teknis

Sebagian besar literatur menunjukkan bahwa faktor manusia tetap menjadi salah satu sumber risiko operasional TI yang signifikan, sehingga mekanisme identifikasinya perlu melibatkan evaluasi prosedur kerja, kompetensi pegawai, dan pola kepatuhan terhadap standar keamanan. Studi Yasirandi, Rakhmatsyah, dan Kurniawan (2021) menegaskan bahwa kesalahan input, ketidaktelitian operator, dan kurangnya pemahaman terhadap sistem menjadi pemicu utama gangguan layanan informasi. Penelitian Hasibuan (2024) pada sektor perbankan syariah juga menjelaskan bahwa risiko operasional sering

muncul dari praktik kerja yang tidak sesuai standar atau kurangnya pengawasan pada unit-unit operasional. Identifikasi risiko yang memasukkan aspek SDM memungkinkan organisasi mengenali sumber ancaman yang tidak sepenuhnya teknis tetapi berdampak besar pada operasi layanan.

Pemanfaatan teknologi informasi sebagai alat identifikasi risiko operasional tercermin dalam beberapa penelitian yang menyoroti peran sistem pemantauan real-time dan analitik data sebagai metode identifikasi modern. Lubis, Lestari, Harahap, dan Arsyadona (2025) mengemukakan bahwa teknologi mempunyai kapasitas untuk mendeteksi pola abnormal yang mengindikasikan potensi risiko operasional melalui pemrosesan data yang cepat dan akurat. Kajian Luo et al. (2023) menunjukkan bahwa logika fuzzy dan neural network dapat membantu mengidentifikasi risiko berbasis pola ketidakpastian pada proses bisnis yang memiliki variabilitas tinggi. Pendekatan teknologi ini memperkaya metode identifikasi tradisional dan membuat organisasi lebih adaptif terhadap dinamika ancaman yang semakin tidak terduga.

Literatur menunjukkan bahwa identifikasi risiko yang efektif memerlukan integrasi antara proses audit TI dan evaluasi berkala terhadap seluruh komponen ekosistem teknologi organisasi. Fuji, Supriadi, dan Junaedi (2025) menegaskan bahwa audit yang dilakukan secara menyeluruh membantu menemukan celah risiko yang tidak terdeteksi melalui pengamatan rutin. Settembre-Blundo et al. (2021) menambahkan bahwa organisasi perlu menerapkan sistem manajemen risiko yang fleksibel agar dapat mengidentifikasi ancaman saat lingkungan operasional mengalami ketidakpastian. Pendekatan audit terpadu menghasilkan proses identifikasi risiko yang lebih akurat dan mendukung pengambilan keputusan berbasis bukti.

Dalam penelitian terkait rantai pasokan global, identifikasi risiko operasional TI dilakukan melalui pemetaan alur informasi, pemahaman hubungan antar-entitas, dan evaluasi kemungkinan gangguan pada titik pertukaran data. Kajian Mardikaningsih et al. (2024) menunjukkan bahwa gangguan teknologi informasi di sepanjang rantai pasokan dapat memunculkan risiko operasional berskala besar yang berdampak pada kelancaran logistik. Fernando et al. (2023) menemukan bahwa dalam ekosistem industri 4.0, identifikasi risiko perlu menilai keamanan sistem cyber supply chain untuk mencegah gangguan proses produksi. Pentingnya mengidentifikasi kerentanan pada titik distribusi informasi membuat mekanisme identifikasi risiko TI semakin strategis dalam manajemen operasional global.

Penguatan sistem identifikasi risiko juga tercermin dalam literatur yang membahas standar keamanan OT (*Operational Technology*) yang digunakan untuk memastikan keandalan sistem industri. Stouffer et al. (2023) menekankan bahwa identifikasi risiko pada OT membutuhkan pendekatan analitis terhadap aset, jalur serangan, dan kemungkinan eksposur dari perangkat yang terhubung. Penelitian Girling (2022) menunjukkan bahwa sektor perbankan dan fintech memerlukan teknik identifikasi yang mampu menangkap risiko operasional lintas platform digital, terutama pada sistem pembayaran elektronik. Identifikasi risiko yang semakin terperinci membantu organisasi mengelola ancaman operasional yang bergerak cepat dan bervariasi.

Penilaian Risiko Operasional TI

Penilaian risiko operasional TI dalam berbagai literatur dipahami sebagai proses sistematis untuk menentukan tingkat keparahan suatu risiko melalui analisis kemungkinan terjadinya insiden serta besarnya dampak yang dapat ditimbulkannya terhadap proses operasional organisasi. Kajian Asmarawati dan Dewi (2024) menjelaskan bahwa penilaian risiko harus didukung data historis, indikator kinerja, dan catatan gangguan yang dapat menggambarkan perilaku risiko secara objektif. Proses penilaian ini tidak hanya menilai aspek teknis pada sistem informasi, tetapi juga mempertimbangkan kesiapan organisasi dalam merespons potensi ancaman. Tingkat keakuratan penilaian risiko sangat dipengaruhi oleh kualitas proses identifikasi yang telah dilakukan sebelumnya.

Dalam penelitian Ricky (2017), penilaian risiko operasional TI memerlukan pendekatan kuantitatif untuk menghitung kemungkinan kegagalan perangkat keras atau perangkat lunak berdasarkan frekuensi terjadinya gangguan dalam periode tertentu. Perhitungan probabilitas dan estimasi dampak memungkinkan organisasi memahami prioritas mitigasi yang harus dilakukan untuk mencegah gangguan layanan yang berulang. Kajian tersebut juga menegaskan bahwa pemeringkatan risiko menjadi poin penting agar organisasi dapat mengalokasikan sumber daya secara tepat ke area yang memiliki tingkat ancaman paling kritis. Pendekatan matematis ini memberikan struktur yang jelas bagi pengambil keputusan dalam menetapkan prioritas penanganan risiko.

Berbagai studi dalam kajian Parera et al. (2022) menunjukkan bahwa penilaian risiko pada sektor kesehatan sering kali mempertimbangkan kerentanan data, kualitas sistem rekam medis digital, dan potensi kehilangan informasi sebagai risiko operasional utama. Pada konteks tersebut, penilaian risiko tidak hanya menghitung kemungkinan gangguan teknis, tetapi juga memperhitungkan konsekuensi regulasi dan implikasi etis terkait kerahasiaan informasi. Mengintegrasikan analisis risiko teknis dan nonteknis memungkinkan organisasi kesehatan menilai tingkat ancaman dengan lebih komprehensif. Penilaian risiko yang matang membantu meminimalkan kesalahan operasional yang berdampak pada keselamatan pasien.

Kerangka COBIT 5 yang dibahas dalam studi Thenu, Wijaya, dan Rudianto (2020) menawarkan pendekatan penilaian risiko yang berfokus pada domain proses TI sehingga menghasilkan evaluasi risiko yang lebih terarah. Dalam kerangka ini, tingkat risiko dinilai berdasarkan keefektifan kontrol yang diterapkan pada setiap proses operasional TI dan seberapa besar kesenjangan antara kondisi ideal dengan praktik aktual. Penelitian Nisa', Febrianti, dan Ajrina (2023) menunjukkan bahwa organisasi yang menerapkan COBIT mampu melakukan penilaian risiko lebih konsisten karena setiap aktivitas memiliki indikator pengukuran yang terstandar. Pendekatan berbasis kontrol ini membuat penilaian risiko lebih berbasis fakta dan tidak bergantung pada persepsi subjektif auditor.

Perkembangan teknologi berbasis AI dan big data memberi kontribusi besar dalam memperkuat akurasi penilaian risiko operasional TI, khususnya melalui kemampuan model prediktif dalam mengestimasi pola ancaman yang sulit ditangkap secara manual. Studi Caseba dan Dewayanto (2024) menegaskan bahwa teknik prediksi berbasis data mampu memberikan peringatan dini terkait ancaman penipuan digital yang memiliki pola serangan kompleks. Kajian Santorry (2024) juga menemukan bahwa teknologi finansial membutuhkan penilaian risiko berbasis analitik untuk mengukur dampak potensi gangguan otomatisasi dan kesalahan algoritma. Kehadiran teknologi tersebut memperkaya metode penilaian dan memungkinkan organisasi membuat keputusan mitigasi yang lebih tajam.

Literatur menunjukkan bahwa penilaian risiko operasional TI juga membutuhkan evaluasi terhadap kesiapan sumber daya manusia sebagai bagian integral dari kerentanan operasional. Penelitian Yasirandi, Rakhmatsyah, dan Kurniawan (2021) menjelaskan bahwa tingkat kompetensi, disiplin prosedural, dan konsistensi pegawai dalam mengikuti standar operasional turut menentukan besarnya risiko yang mungkin timbul. Dalam sektor perbankan syariah, sebagaimana dijelaskan oleh Hasibuan (2024), penilaian risiko operasional mengharuskan organisasi mengukur dampak kesalahan manusia terhadap kualitas layanan digital. Dengan mempertimbangkan faktor manusia, hasil penilaian risiko menjadi lebih akurat dan relevan dengan kondisi operasional sehari-hari.

Penilaian risiko berbasis audit teknologi juga mendapat sorotan dalam literatur, terutama pada penelitian Fuji, Supriadi, dan Junaedi (2025) yang menekankan bahwa audit mendalam dapat menilai efektivitas kontrol TI dibandingkan sekadar mengidentifikasi keberadaannya. Audit yang dilakukan secara berkala memungkinkan organisasi mengukur stabilitas sistem, mendeteksi degradasi performa, serta menentukan seberapa besar risiko yang masih perlu mendapat intervensi manajemen. Pendekatan ini juga diperlukan untuk memastikan bahwa kontrol yang dirancang tetap berfungsi saat organisasi mengalami perubahan proses atau melakukan adopsi teknologi baru. Dengan demikian, audit TI berperan penting dalam membentuk hasil penilaian risiko yang valid.

Penilaian risiko operasional TI memerlukan analisis mendalam terhadap kelancaran arus informasi dan potensi gangguan pada sistem yang menghubungkan berbagai pihak. Kajian Mardikaningsih et al. (2024) menunjukkan bahwa penilaian risiko harus mempertimbangkan kebergantungan antara proses logistik dan teknologi informasi yang digunakan untuk memantau pergerakan barang. Sementara itu, penelitian Fernando et al. (2023) menegaskan bahwa dalam ekosistem industri 4.0, penilaian risiko harus melibatkan evaluasi terhadap keamanan pertukaran data antar-sistem produksi. Hal ini membuat penilaian risiko semakin penting karena gangguan TI mampu menghambat operasi rantai pasokan secara keseluruhan.

Sektor teknologi operasional (OT) juga memberikan gambaran bahwa penilaian risiko perlu memperhitungkan eksposur perangkat industri terhadap ancaman serangan maupun kegagalan sistemik. Stouffer et al. (2023) menegaskan bahwa untuk menilai risiko OT, organisasi perlu menilai kondisi aset, kemungkinan jalur serangan, serta keandalan infrastruktur yang menghubungkan perangkat-perangkat tersebut. Kajian Girling (2022) juga menyoroti bahwa sektor keuangan digital membutuhkan penilaian risiko yang dapat mengukur ancaman lintas platform dan potensi gangguan layanan pembayaran

elektronik. Penilaian risiko dalam konteks OT dan keuangan digital menegaskan pentingnya memahami karakteristik operasional masing-masing sistem.

Hasil kajian literatur menunjukkan bahwa penilaian risiko operasional TI tidak dapat dilakukan dengan satu pendekatan tunggal, melainkan memerlukan kombinasi antara metode kuantitatif, kualitatif, audit, serta analisis berbasis teknologi. Setiap sektor memiliki parameter risiko yang berbeda sehingga penilaian harus menyesuaikan karakteristik proses dan skala operasional. Proses penilaian yang matang memberikan dasar kuat bagi organisasi dalam menentukan strategi mitigasi yang efektif dan mengalokasikan sumber daya dengan tepat, sehingga kualitas penilaian risiko menjadi faktor penentu keberhasilan seluruh rangkaian manajemen risiko operasional TI.

Dampak Risiko Operasional TI terhadap Manajemen Risiko

Dampak risiko operasional TI terhadap manajemen risiko organisasi terlihat dari meningkatnya kebutuhan untuk memperkuat struktur pengawasan serta ketepatan mekanisme kontrol yang mampu menahan gangguan sistemik secara berkelanjutan. Studi Sipior, Lombardi, dan Gabryelczyk (2021) memperlihatkan bahwa insiden pada sistem informasi dapat memicu gangguan operasional berantai yang merusak stabilitas proses bisnis inti. Organisasi yang menghadapi gangguan TI tanpa persiapan memadai cenderung mengalami keterlambatan operasional, meningkatnya biaya pemulihan, dan menurunnya kepercayaan pengguna. Situasi tersebut menegaskan bahwa risiko TI bukan sekadar masalah teknis, melainkan faktor yang menentukan ketahanan operasional secara menyeluruh.

Dalam manajemen risiko, gangguan yang berasal dari sistem TI berkaitan erat dengan penurunan efektivitas pengambilan keputusan karena data yang digunakan manajer menjadi tidak lengkap atau tidak dapat diakses ketika sistem mengalami kerusakan. Penelitian Thenu, Wijaya, dan Rudianto (2020) menunjukkan bahwa kegagalan TI dapat memengaruhi seluruh siklus proses bisnis, mulai dari input, pemrosesan, hingga pengiriman layanan kepada pengguna akhir. Ketidakstabilan ini berimplikasi langsung pada menurunnya kemampuan organisasi merespons ancaman secara cepat dan terukur. Dampak tersebut mendorong manajer risiko untuk meningkatkan investasi dalam kontrol dan pemantauan TI yang lebih kuat.

Kerugian finansial menjadi salah satu dampak paling menonjol dari risiko operasional TI yang tidak terkendali, sebagaimana dibahas dalam kajian Capriani dan Dana (2016) pada sektor perbankan. Gangguan TI dapat menyebabkan tertundanya transaksi, kegagalan pemrosesan data, dan meningkatnya biaya operasional akibat kebutuhan perbaikan sistem secara berulang. Selain itu, organisasi menghadapi tekanan regulasi ketika gangguan TI membuka potensi terjadinya pelanggaran terhadap standar keamanan dan kerahasiaan data. Hal tersebut membuat manajemen risiko harus memasukkan skenario kerugian finansial ke dalam perhitungan perencanaan ketahanan operasional.

Risiko operasional TI juga berdampak pada reputasi organisasi, terutama ketika layanan digital yang digunakan pelanggan mengalami gangguan berulang atau menunjukkan ketidakandalan yang mengurangi tingkat kepuasan pengguna. Studi Santorry (2024) menunjukkan bahwa industri keuangan modern sangat sensitif terhadap kegagalan sistem karena pelanggan mengharapkan kecepatan, akurasi, dan stabilitas layanan digital. Kegagalan tersebut tidak hanya memengaruhi kepercayaan pelanggan, tetapi juga menurunkan posisi kompetitif perusahaan di pasar digital. Oleh sebab itu, manajemen risiko harus mempertimbangkan reputasi sebagai dimensi dampak yang memiliki kontribusi signifikan terhadap keberlangsungan organisasi.

Risiko operasional yang tidak terkelola dalam sektor proyek teknologi informasi dapat menyebabkan keterlambatan implementasi, pembengkakan biaya, dan penurunan kualitas hasil proyek. Sitorus, Maria, dan Safa (2024) menjelaskan bahwa ancaman siber, kegagalan integrasi sistem, dan kurangnya dokumentasi teknis sering kali memperpanjang fase pengembangan dan pengujian. Dampak tersebut mempengaruhi manajer proyek dalam menyusun strategi mitigasi yang lebih terstruktur agar risiko tidak menyebar ke fase operasional setelah proyek selesai. Dengan demikian, risiko operasional TI memiliki keterkaitan langsung dengan keberhasilan proyek dan efektivitas manajemen risiko jangka panjang.

Pada instansi pemerintahan, seperti yang dikaji Sutigar et al. (2024), risiko operasional TI berdampak besar pada konsistensi pelayanan publik yang sangat bergantung pada sistem informasi. Ketidakstabilan TI dapat menghambat proses administrasi, memperlambat layanan masyarakat, serta menurunkan akurasi data yang menjadi dasar perumusan kebijakan. Dampak tersebut memperkuat urgensi penerapan kerangka manajemen risiko yang terstruktur untuk menjaga kelancaran fungsi

pemerintahan. Tanpa kontrol TI yang memadai, risiko teknis dapat berkembang menjadi risiko organisasi yang lebih luas.

Studi Ahkmad (2024) menyoroti bahwa risiko operasional TI dapat memperlemah kemampuan organisasi dalam mempertahankan tingkat kepatuhan terhadap standar ISO 31000, terutama ketika kontrol yang disyaratkan tidak berfungsi optimal. Ketika organisasi gagal memenuhi standar tersebut, kualitas tata kelola risiko secara keseluruhan akan menurun dan mengekspos organisasi terhadap ancaman yang lebih sulit dikendalikan. Situasi ini menuntut manajemen risiko untuk terus memperbarui skema kontrol guna menutup celah operasional yang muncul akibat perubahan teknologi. Dengan kata lain, risiko TI memiliki dampak struktural yang langsung mempengaruhi maturitas manajemen risiko.

Gangguan pada teknologi informasi dalam sistem rantai pasokan global dapat menciptakan efek domino terhadap alur logistik, koordinasi vendor, dan kecepatan distribusi barang. Kajian Mardikaningsih et al. (2024) memperlihatkan bahwa risiko TI mampu menghambat proses pelacakan dan pelaporan, yang pada akhirnya mengganggu pengambilan keputusan strategis dalam rantai pasokan. Dampak tersebut menegaskan bahwa risiko operasional TI tidak dapat dipisahkan dari strategi mitigasi risiko logistik dan manajemen hubungan antar organisasi. Oleh sebab itu, integrasi antara manajemen risiko operasional TI dan manajemen rantai pasokan menjadi kebutuhan strategis.

Budianto (2023) menegaskan bahwa dalam industri keuangan, risiko operasional TI berdampak pada konsentrasi eksposur risiko lintas proses, terutama pada aktivitas berbasis digital yang memiliki sensitivitas tinggi terhadap gangguan teknis. Ketika konsentrasi risiko meningkat, manajemen risiko harus mengalokasikan sumber daya lebih besar untuk memantau titik kritis guna menekan potensi kegagalan yang dapat mengganggu operasional. Risiko yang tidak terkendali dapat mengubah profil risiko organisasi secara keseluruhan dan menyebabkan perubahan signifikan pada kebijakan mitigasi. Dalam konteks ini, risiko TI memiliki kontribusi langsung terhadap dinamika profil risiko perusahaan.

Dampak risiko operasional TI menunjukkan bahwa manajemen risiko modern tidak dapat berdiri tanpa fondasi pengendalian TI yang kuat dan berkelanjutan. Risiko TI memengaruhi stabilitas operasional, kualitas layanan, integritas data, reputasi, efisiensi biaya, dan kepatuhan regulasi, sehingga meningkatkan kompleksitas pengelolaan risiko di berbagai sektor. Dampak tersebut mendorong organisasi untuk memasukkan TI sebagai komponen inti dalam desain strategi manajemen risiko jangka panjang, sehingga risiko operasional TI menjadi faktor strategis yang membentuk ketahanan organisasi di era digital.

KESIMPULAN

Penelitian ini menunjukkan bahwa risiko operasional dalam teknologi informasi memiliki implikasi yang signifikan terhadap keberlangsungan operasional organisasi, terutama ketika sistem digital menjadi fondasi utama proses bisnis. Melalui kajian literatur yang komprehensif, ditemukan bahwa mekanisme identifikasi risiko harus dilakukan secara sistematis dengan menggabungkan analisis proses bisnis, audit teknologi, pemantauan berbasis data, serta evaluasi sumber daya manusia untuk memperoleh gambaran menyeluruh mengenai titik kerentanan operasional. Penilaian risiko operasional TI memerlukan pendekatan integratif yang melibatkan metode kuantitatif, kualitatif, teknologi prediktif, serta kerangka kontrol seperti ISO 31000 dan COBIT agar organisasi mampu menentukan prioritas mitigasi yang paling relevan dan efektif.

Dampak risiko operasional TI terhadap manajemen risiko terbukti bersifat multidimensional, mulai dari kerugian finansial, gangguan layanan, penurunan reputasi, hingga hambatan dalam pengambilan keputusan strategis ketika sistem informasi tidak stabil. Literatur menunjukkan bahwa risiko TI bukan hanya isu teknis, tetapi komponen strategis yang mempengaruhi ketahanan organisasi secara keseluruhan. Dengan demikian, pengelolaan risiko operasional TI harus menjadi bagian esensial dari kerangka manajemen risiko korporasi, sehingga perusahaan dapat mempertahankan stabilitas, meningkatkan kualitas layanan digital, serta meminimalkan eksposur terhadap ancaman yang terus berkembang di era transformasi digital.

DAFTAR PUSTAKA

Ahkmad, F. F. (2024). Manajemen Risiko dalam Optimalisasi Keberhasilan Proyek Teknologi Informasi Menggunakan Framework ISO 31000. *Jurnal Telematika*, *19*(2), 60-64. https://doi.org/10.61769/telematika.v19i2.712.

Asmarawati, S. G., & Dewi, A. M. (2024). Asesmen Manajemen Risiko Berdasarkan ISO 31000 dalam Pengukuran Risiko Operasional dan Risiko Keuangan pada Perusahaan XYZ. *JEBDEKER: Jurnal Ekonomi, Manajemen, Akuntansi, Bisnis Digital, Ekonomi Kreatif, Entrepreneur*, 4(2), 365–388. https://doi.org/10.56456/jebdeker.v4i2.267

Budianto, E. W. H. (2023). Pemetaan penelitian risiko operasional pada industri keuangan syariah dan konvensional: studi bibliometrik VosViewer dan literature review. *Jurnal Ekonomi Islam*, *14*(2), 158-174.

Capriani, N., & Dana, I. (2016). Pengaruh Risiko Kredit Risiko Operasional Dan Risiko Likuiditas Terhadap Profitabilitas BPR Di Kota Denpasar. *E-Jurnal Manajemen*, 5(3), 1486–1512. https://ojs.unud.ac.id/index.php/manajemen/article/view/16316

Caseba, F. L., & Dewayanto, T. (2024). Penerapan Artificial Intelligence, Big Data, Dan Blockchain Dalam Fintech Payment Terhadap Risiko Penipuan Komputer (Computer Fraud Risk): A Systematic Literature Review. *Diponegoro Journal Of Accounting*, 13(3), 1–15 https://ejournal3.undip.ac.id/index.php/accounting/article/view/46058

Chowdhury, S., Rodriguez-Espindola, O., Dey, P., & Budhwar, P. (2023). Blockchain technology adoption for managing risks in operations and supply chain management: evidence from the UK. *Annals of operations research*, *327*(1), 539-574. https://doi.org/10.1007/s10479-021-04487-1.

Cisco, *Cybersecurity Readiness Index 2025*: "86% perusahaan global melaporkan insiden keamanan terkait AI dalam 12 bulan terakhir". Link: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m05/cisco-study-reveals-alarming-deficiencies-in-security-readiness.html Cisco Newsroom+1

El Hajj, M., & Hammoud, J. (2023). Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk management, and financial operations. *Journal of Risk and Financial Management*, *16*(10), 434. https://doi.org/10.3390/jrfm16100434.

Fernando, Y., Tseng, M. L., Wahyuni-Td, I. S., de Sousa Jabbour, A. B. L., Chiappetta Jabbour, C. J., & Foropon, C. (2023). Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia. *Journal of Industrial and Production Engineering*, *40*(2), 102-116. https://doi.org/10.1080/21681015.2022.2116495.

Fuji, S. (2025). Strategi Manajemen Risiko Teknol Strategi Manajemen Risiko Teknologi Informasi Berbasis Studi Literatur. *TeIKa*, *15*(1).

Fuji, S., Supriadi, F., & Junaedi, I. D. (2025). Strategi Manajemen Risiko Teknol Strategi Manajemen Risiko Teknologi Informasi Berbasis Studi Literatur. *Teika,* 15(1). https://jurnal.unai.edu/index.php/teika/article/view/3838

Girling, P. X. (2022). *Operational risk management: a complete guide for banking and fintech*. John Wiley & Sons.

Habsy, B. A. (2017). Seni Memehami Penelitian Kuliatatif Dalam Bimbingan Dan Konseling : Studi Literatur. *JURKAM: Jurnal Konseling Andi Matappa*, 90–100. https://doi.org/10.31100/jurkam.v1i2.56

Habsy, B. A., Mufidha, N., Shelomita, C., Rahayu, I., & Muckorobin, Moch. I. (2023). Filsafat Dasar Dalam Konseling Psikoanalisis : Studi Literatur. *Indonesian Journal Of Educational Counseling*, 7(2), 189–199. https://doi.org/10.30653/001.202372.266

Hasibuan, R. P. A. (2024). Manajemen Risiko Operasional pada Bank Syariah Indonesia (BSI) KC Bengkulu. *EKOMA: Jurnal Ekonomi, Manajemen, Akuntansi*, 3(4), 879-891. https://ulilalbabinstitute.co.id/index.php/EKOMA/article/view/3377

Judijanto, L., Hindarto, D., Wahjono, S. I., & Djunarto, A. (2023). Edge of enterprise architecture in addressing cyber security threats and business risks. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(3), 386-396.

Lubis, N. A. S. F., Lestari, D., Harahap, U. Y., & Arsyadona. (2025). Peran Teknologi Informasi Dalam Mengelola Risiko Operasional. *Kohesi: Jurnal Multidisiplin Saintek*, *6*. https://doi.org/10.8734/Kohesi.v1i2.365

Luo, N., Yu, H., You, Z., Li, Y., Zhou, T., Jiao, Y., ... & Qiao, S. (2023). Fuzzy logic and neural network-based risk assessment model for import and export enterprises: A review. *Journal of*

Data Science and Intelligent Systems, *1*(1), 2-11. https://doi.org/10.47852/bonviewJDSIS32021078.

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.

Nisa', F. Z., Febrianti, G. D., & Ajrina, N. N. (2023). Systematic Literature Review: Analisis Implementasi Manajemen Risiko TI Menggunakan Framework COBIT di Sektor Industri Jasa. *Bulletin of Computer Science Research*, *4*(1), 66–74. https://doi.org/10.47065/bulletincsr.v4i1.313

Parera, M. F., Indawati, L., Rumana, N. A., & Yulia, N. (2022). Manajemen Risiko Di Ruang Penyimpanan Rekam Medis (Literature Review) . *Journal Of Innovation Research And Knowledge*, 1(10), 1323–1326. https://doi.org/10.53625/jirk.v1i10.1744

PwC, *Global Digital Trust Insights Survey* (2022): "27% organisasi mengalami pelanggaran data dengan biaya US$ 1-20 juta dalam 3 tahun terakhir". Link: https://www.pwc.com/bm/en/press-releases/global-digital-trust-insights-survey.html PwC+1

PwC, *Global Risk Survey 2023*. "37% organisasi merasa sangat terekspos terhadap risiko siber". Link: https://www.pwc.com/id/en/media-centre/press-release/2024/indonesian/pwc-global-risk-survey-2023.html PwC+1

Rahmatika, A. N., Apriyadi, M. F., Kahfi, M A., & Aibi, O. N. (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

Ricky (2017). Analisis Risiko Operasional Dalam Pemilihan Perangkat Keras (Hardware) Dan Perangkat Lunak (Software) Pada Industri Perbankan (Studi Kasus: Bank X). *Jurnal Ekonomi, Manajemen Dan Perbankan (Journal of Economics, Management and Banking)*, *1*(2), 43. https://doi.org/10.35384/jemp.v1i2.36

Salamai, A. A., El-kenawy, E. S. M., & Abdelhameed, I. (2021). Dynamic voting classifier for risk identification in supply chain 4.0. *Computers, Materials & Continua*, *69*(3).

Santorry, S. (2024). Evaluating the Impact of Technological Innovations on Operational Risk Management in Financial Institutions. *The Journal of Academic Science*, *1*(6), 762-776. https://doi.org/10.59613/7hgzeg07.

Setiawan, R., & Rahmadsyah. (2025). Digitalisasi Perbankan dan Ancaman Keamanan Siber: Tantangan dan Strategi Mitigasi Risiko Operasional. *ASEFBA: Advanced Studies in Economic, Finance and Banking*, *1*(1), 73–87. https://journalweb.org/ojs/index.php/ASEFBA/article/view/548

Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., & García-Muiña, F. E. (2021). Flexibility and resilience in corporate decision making: a new sustainability-based risk management system in uncertain times. *Global Journal of Flexible Systems Management*, *22*(Suppl 2), 107-132. https://doi.org/10.1007/s40171-021-00277-7.

Sipior, J. C., Lombardi, D. R., & Gabryelczyk, R. (2021). Information technology operational risk: A teaching case. *Journal of Computer Information Systems*, *61*(4), 328-344. https://doi.org/10.1080/08874417.2019.1647767.

Sirait, N. M., & Susanty, A. (2016). Analisis Risiko Operasional Berdasarkan Pendekatan Enterprise Risk Management (Erm) Pada Perusahaan Pembuatan Kardus Di Cv Mitra Dunia Palletindo. *Industrial Engineering Online Journal*, 5(4), 1–10. https://ejournal3.undip.ac.id/index.php/ieoj/article/view/14043

Sitorus, M. G. B., Maria, N., & Safa, Y. N. (2024). Tinjauan Literatur Manajemen Risiko Cyber dalam Proyek: Identifikasi, Evaluasi, dan Mitigasi Ancaman. *Jurnal Manajemen Informatika (JAMIKA)*, *14*(2), 187-198. https://doi.org/10.34010/jamika.v14i2.12887.

Stouffer, K., Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., ... & Thompson, M. (2023). Guide to operational technology (ot) security.

Sutigar, M. B. B., Bhisma, V. A., Firmansyah, A. N., & Wulansari, A. (2024). Studi Literature Review IT Risk Management di Instansi Pemerintahan. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(1), 75-79. https://doi.org/10.36040/jati.v8i1.8734.

Syadali, M. R. A., Segaf, S., & Parmujianto, P. (2023). Risk management strategy for the problem of borrowing money for Islamic commercial banks. *Enrichment: Journal of Management*, *13*(2), 1227-1236. https://doi.org/10.35335/enrichment.v13i2.1392.

Thenu, P. P., Wijaya, A. F., & Rudianto, C. (2020). Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus: Pt Global Infotech). *Jurnal Bina Komputer*, *2*(1), 1–13. https://doi.org/10.33557/binakomputer.v2i1.799

Yasirandi, R., Rakhmatsyah, A., & Kurniawan, F. (2021). IT Risk Management dalam Operasional untuk Peningkatan Layanan Informasi Pesanan. *Krea-TIF*, *9*(2), 21. https://doi.org/10.32832/kreatif.v9i2.5982.