Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

Optimalisasi Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 di Era Digital

Muhammad Rifqi Naufal Irsyad[1], Ilham[2]

Program Studi Sistem Informasi[1,2]
Fakultas Sains dan Teknologi[1,2]
Universitas Islam Negeri Sunan Ampel Surabaya[1,2]

rifqii.naufall37@gmail.com[1], ilham@uinsa.ac.id[2]

Received: 2024-11-21**. Revised:** 2024-12-27**. Accepted:** 2024-12-29**.**
Issue Period: Vol.9 No.1 (2025), Pp. 24-41

Abstrak: Di era digital, teknologi informasi telah menjadi tulang punggung operasional organisasi, namun juga membawa risiko yang kompleks. Penelitian ini membahas penerapan framework ISO 31000 dalam manajemen risiko teknologi informasi (TI), yang menawarkan pendekatan sistematis untuk mengidentifikasi, menganalisis, dan mengelola risiko. Framework ini tidak hanya meningkatkan ketahanan organisasi terhadap ancaman digital, tetapi juga mendukung integrasi manajemen risiko ke dalam strategi bisnis untuk menciptakan nilai tambah. Melalui studi literatur, penelitian ini mengidentifikasi tantangan utama seperti resistensi budaya, keterbatasan sumber daya, dan kurangnya integrasi strategi. Solusi yang diusulkan mencakup sosialisasi, pelatihan, dan penggunaan teknologi seperti big data dan kecerdasan buatan untuk memperkuat efektivitas manajemen risiko.

Kata kunci: manajemen risiko; teknologi informasi; ISO 31000

Abstract: *In the digital era, information technology has become the backbone of organizational operations but also introduces complex risks. This study examines the application of the ISO 31000 framework in IT risk management, offering a systematic approach to identifying, analyzing, and managing risks. The framework not only enhances organizational resilience against digital threats but also supports the integration of risk management into business strategies to create added value. Through a literature review, this study identifies key challenges such as cultural resistance, resource limitations, and strategic integration gaps. Proposed solutions include socialization, training, and leveraging technologies like big data and artificial intelligence to strengthen risk management effectiveness.*

Keywords: *risk management; information technology; ISO 31000*

I. PENDAHULUAN

Dalam konteks perkembangan teknologi informasi yang semakin pesat dan kompleks, manajemen risiko telah muncul sebagai elemen fundamental dalam memastikan keberlanjutan operasional dan daya saing organisasi di berbagai sektor. Transformasi digital yang dihasilkan oleh kemajuan teknologi seperti kecerdasan buatan (AI), Internet of Things (IoT), dan otomatisasi tidak hanya menciptakan peluang baru untuk meningkatkan efisiensi operasional dan mendorong inovasi, tetapi juga menimbulkan tantangan yang signifikan dalam pengelolaan risiko. Organisasi saat ini dihadapkan pada beragam risiko yang muncul akibat

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

ketergantungan mereka terhadap teknologi informasi, termasuk risiko keamanan siber, pelanggaran privasi data, kegagalan sistem, serta tantangan terkait kepatuhan terhadap regulasi yang terus berkembang dan semakin ketat.

Risiko keamanan siber, misalnya, telah menjadi perhatian utama bagi banyak organisasi karena meningkatnya insiden pelanggaran data yang dapat mengakibatkan kerugian finansial yang besar serta kerusakan reputasi yang sulit diperbaiki. Selain itu, pelanggaran privasi data sering kali berujung pada sanksi hukum yang berat dan kehilangan kepercayaan dari pelanggan. Kegagalan sistem TI juga dapat menyebabkan gangguan operasional yang signifikan, mempengaruhi produktivitas dan efisiensi secara keseluruhan. Dalam konteks ini, organisasi perlu menghadapi tantangan untuk mengelola risiko-risiko tersebut dengan pendekatan yang lebih terstruktur dan sistematis.

Penerapan framework ISO 31000 menjadi semakin relevan dalam menghadapi tantangan ini. ISO 31000 menyediakan pedoman yang komprehensif untuk pengelolaan risiko yang dapat diadaptasi oleh organisasi dari berbagai sektor. Framework ini membantu organisasi dalam mengidentifikasi, menilai, dan mengelola risiko secara terintegrasi dengan strategi bisnis mereka. Dengan demikian, ISO 31000 tidak hanya berfungsi sebagai alat untuk mitigasi risiko tetapi juga sebagai panduan untuk menciptakan nilai melalui pengelolaan risiko yang terencana. Penerapan ISO 31000 memungkinkan organisasi untuk membangun kerangka kerja manajemen risiko yang lebih holistik, di mana setiap aspek dari operasi bisnis dipertimbangkan dalam konteks risiko.

Meskipun banyak organisasi telah mengakui pentingnya manajemen risiko, banyak dari mereka masih menggunakan pendekatan yang bersifat reaktif dan terfragmentasi. Dalam banyak kasus, manajemen risiko teknologi informasi dipandang sebagai fungsi pendukung yang terpisah dari keputusan strategis utama. Hal ini menciptakan kesenjangan antara kebijakan manajemen risiko dan praktik operasional sehari-hari, yang dapat mengakibatkan kerentanan terhadap berbagai ancaman digital. Ketidakmampuan untuk mengintegrasikan manajemen risiko TI ke dalam kerangka kerja keseluruhan organisasi sering kali menyebabkan respons yang lambat terhadap insiden keamanan dan kegagalan sistem.

Lebih lanjut, dengan meningkatnya ekspektasi dari pemangku kepentingan termasuk pelanggan, investor, dan regulator terhadap keamanan data dan perlindungan privasi, organisasi dituntut untuk mengembangkan pendekatan manajemen risiko yang lebih komprehensif dan terstruktur. Kegagalan untuk memenuhi ekspektasi ini tidak hanya dapat merugikan reputasi organisasi tetapi juga dapat berdampak langsung pada kepercayaan pelanggan serta keberlangsungan bisnis itu sendiri. Oleh karena itu, penting bagi organisasi untuk memahami bahwa manajemen risiko bukan hanya sekadar kepatuhan terhadap regulasi atau prosedur internal; melainkan merupakan bagian integral dari strategi bisnis mereka [1].

Penelitian ini bertujuan untuk mengeksplorasi bagaimana organisasi dapat mengoptimalkan manajemen risiko teknologi informasi mereka dengan menggunakan framework ISO 31000. Fokus penelitian ini adalah pada tahapan-tahapan kunci dalam pengelolaan risiko TI mulai dari identifikasi hingga evaluasi dan pemantauan yang diharapkan dapat memberikan panduan praktis bagi organisasi dalam meningkatkan ketahanan mereka terhadap ancaman digital. Selain itu, penelitian ini juga akan membahas bagaimana integrasi manajemen risiko TI ke dalam strategi bisnis dapat membantu organisasi tidak hanya untuk bertahan tetapi juga untuk berkembang di tengah ketidakpastian [2].

Melalui analisis penerapan ISO 31000 dalam konteks teknologi informasi, penelitian ini diharapkan dapat memberikan wawasan bagi para pemimpin organisasi dan pengambil keputusan tentang pentingnya pengelolaan risiko yang terintegrasi. Hasil penelitian ini akan relevan bagi sektor-sektor yang sangat bergantung pada teknologi digital seperti perbankan, kesehatan, e-commerce, dan sektor publik di mana volatilitas serta ketidakpastian sering kali mendominasi lanskap bisnis saat ini.

Dengan demikian, penelitian ini bertujuan untuk memberikan pemahaman tentang bagaimana framework ISO 31000 dapat digunakan secara efektif dalam pengelolaan risiko teknologi informasi. Melalui pendekatan yang lebih terstruktur dan sistematis ini, diharapkan penelitian ini dapat memberikan kontribusi pada praktik manajemen risiko di berbagai organisasi dengan cara yang lebih pragmatis dan aplikatif. Penelitian ini akan mengeksplorasi langkah-langkah konkret dalam implementasi ISO 31000 serta tantangan-tantangan yang mungkin dihadapi oleh organisasi selama proses tersebut. Dengan demikian, hasil penelitian diharapkan dapat menjadi referensi bagi organisasi dalam merumuskan strategi pengelolaan risiko TI yang lebih efektif di era digital saat ini.

II. LITERATURE REVIEW

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

Tinjauan pustaka ini menyajikan analisis mendalam mengenai penerapan manajemen risiko teknologi informasi dengan menggunakan framework ISO 31000. Berbagai penelitian yang telah dilakukan memberikan wawasan penting mengenai identifikasi, analisis, dan penanganan risiko dalam konteks teknologi informasi di berbagai organisasi.

Penelitian pertama berfokus pada analisis manajemen risiko teknologi informasi dalam aplikasi AHO Office yang digunakan oleh PT. SAT [3]. Penelitian ini bertujuan untuk mengidentifikasi dan mendokumentasikan berbagai jenis risiko yang mungkin terjadi serta cara penanganannya dengan menggunakan framework ISO 31000. Melalui metode kualitatif yang melibatkan wawancara dan observasi langsung, peneliti menemukan total 19 risiko, di mana 3 di antaranya dikategorikan sebagai risiko ekstrem, 7 sebagai risiko tinggi, dan sisanya sebagai risiko sedang hingga rendah. Temuan ini memberikan gambaran yang jelas tentang pentingnya dokumentasi manajemen risiko untuk membantu pemangku kebijakan dalam menyusun strategi mitigasi yang efektif.

Selanjutnya, penelitian yang bertujuan untuk mengevaluasi penerapan framework ISO 31000 pada sistem Tracer Study di Universitas Sebelas April [4]. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif untuk memahami proses bisnis dan struktur organisasi. Dalam penelitian ini, peneliti melakukan identifikasi risiko melalui observasi dan wawancara dengan admin sistem. Proses manajemen risiko dimulai dengan identifikasi, dilanjutkan dengan analisis dan evaluasi risiko berdasarkan frekuensi kejadian serta dampaknya. Penelitian ini menunjukkan bahwa penerapan strategi penanganan risiko yang tepat, seperti monitoring real-time dan pelatihan pengguna, dapat meningkatkan keamanan dan kinerja operasional sistem.

Selanjutnya dalam penelitian mereka tentang implementasi manajemen risiko berbasis ISO 31000 di PT. Schlumberger Geophysics Nusantara mengidentifikasi 14 jenis risiko dalam operasional teknologi informasi perusahaan. Metode analisis deskriptif digunakan untuk mengumpulkan data dari 20 karyawan Divisi IT [5]. Hasil penelitian menunjukkan bahwa 11 dari 14 jenis risiko berada pada level tinggi, sementara 3 lainnya berada pada level moderat. Penelitian ini menekankan pentingnya pemahaman yang mendalam tentang kemungkinan risiko yang dihadapi organisasi serta tindakan yang perlu diambil untuk meningkatkan efektivitas pengelolaan risiko.

Dalam penelitian lain membahas manajemen risiko TI menggunakan kombinasi framework ISO 31000 dan COBIT 5 serta metode Failure Mode and Effects Analysis (FMEA) di PT. XYZ [6]. Penelitian ini menyoroti pentingnya penggabungan beberapa framework dalam pengelolaan risiko untuk meningkatkan efektivitas identifikasi dan penanganan risiko. Penelitian ini menunjukkan bahwa penggunaan COBIT 5 dapat memperkuat proses pengkajian risiko melalui FMEA, memberikan ilustrasi yang jelas mengenai alur pengelolaan risiko yang terintegrasi.

Penelitian oleh Setiawan et al. (2021) juga menyoroti integrasi antara ISO 31000 dan standar keamanan informasi lainnya dalam meningkatkan efektivitas pengelolaan risiko TI di Tripio Purwokerto [7]. Penelitian ini menunjukkan bahwa kombinasi antara berbagai standar dapat memberikan pendekatan yang lebih komprehensif dalam pengelolaan risiko.

Dari literatur yang ada, terlihat bahwa meskipun banyak penelitian telah dilakukan mengenai penerapan framework ISO 31000 dalam manajemen risiko teknologi informasi, masih terdapat celah signifikan dalam literatur terkait integrasi manajemen risiko TI ke dalam strategi bisnis secara menyeluruh. Banyak studi sebelumnya lebih fokus pada identifikasi dan analisis risiko tanpa memberikan panduan praktis tentang bagaimana mengintegrasikan hasil tersebut ke dalam kebijakan strategis organisasi secara efektif. Oleh karena itu, penelitian ini bertujuan untuk mengeksplorasi langkah-langkah konkret dalam pengelolaan risiko TI menggunakan framework ISO 31000, serta memberikan panduan bagi organisasi untuk meningkatkan ketahanan mereka terhadap ancaman digital melalui pendekatan yang lebih terstruktur dan sistematis.

III. METODOLOGI PENELITIAN

Metodologi penelitian ini dirancang untuk mengeksplorasi penerapan framework ISO 31000 dalam manajemen risiko teknologi informasi (TI) di berbagai organisasi. Salah satu komponen kunci dari metodologi ini adalah pemilihan studi literatur sebagai pendekatan utama dalam pengumpulan dan analisis data. Pemilihan studi literatur dilakukan dengan alasan yang kuat, yang akan dijelaskan secara rinci dalam bagian ini.

Studi literatur dipilih karena memberikan dasar yang kokoh untuk memahami konteks dan perkembangan terkini dalam bidang manajemen risiko TI. Dengan meninjau berbagai sumber yang relevan, peneliti dapat

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

mengidentifikasi tren, tantangan, dan praktik terbaik yang telah diterapkan oleh organisasi lain dalam pengelolaan risiko TI. Studi literatur tidak hanya berfungsi sebagai ringkasan dari penelitian sebelumnya, tetapi juga sebagai landasan teoretis yang memperkuat argumen dan metodologi penelitian [8].

Salah satu alasan utama pemilihan studi literatur adalah untuk mengidentifikasi kesenjangan penelitian yang ada. Dalam banyak kasus, meskipun telah ada berbagai penelitian tentang penerapan ISO 31000 dalam manajemen risiko, masih terdapat area yang kurang diteliti, terutama terkait integrasi manajemen risiko TI ke dalam strategi bisnis secara keseluruhan. Dengan mengetahui kesenjangan ini, peneliti dapat merumuskan pertanyaan penelitian yang relevan dan memberikan kontribusi baru dalam bidang tersebut. Selain itu, studi literatur juga membantu peneliti untuk memahami konteks teoretis dan praktis dari topik yang sedang diteliti, sehingga memungkinkan peneliti untuk menempatkan penelitian mereka dalam konteks yang lebih luas.

Proses pelaksanaan studi literatur dalam penelitian ini melibatkan beberapa langkah penting. Pertama, peneliti akan melakukan pencarian sistematis terhadap sumber-sumber informasi yang relevan, termasuk jurnal ilmiah, buku, laporan industri, dan dokumen kebijakan. Kedua, peneliti akan mengevaluasi kualitas dan relevansi setiap sumber informasi untuk memastikan bahwa data yang digunakan adalah akurat dan dapat dipercaya. Ketiga, peneliti akan mensintesis dan menganalisis literatur yang telah dipilih dengan cara mengidentifikasi pola-pola umum, temuan-temuan penting, serta perbedaan di antara studi-studi tersebut.

Melalui proses studi literatur yang sistematis ini, peneliti tidak hanya mendapatkan pemahaman mendalam tentang penerapan framework ISO 31000 tetapi juga dapat mengembangkan kerangka konseptual untuk penelitian mereka sendiri. Dengan meninjau berbagai studi sebelumnya mengenai manajemen risiko TI, peneliti dapat menentukan metode-metode terbaik untuk diterapkan dalam konteks organisasi mereka.

Lebih jauh lagi, studi literatur juga berfungsi untuk mendukung argumen penelitian dengan memberikan bukti pendukung bagi hipotesis atau pertanyaan penelitian yang diajukan. Dengan menunjukkan bagaimana penelitian ini relevan dengan studi-studi sebelumnya, peneliti dapat meyakinkan pembaca tentang kepentingan dan signifikansi dari penelitian yang dilakukan.

Secara keseluruhan, pemilihan studi literatur sebagai bagian dari metodologi penelitian ini sangat penting untuk membangun dasar teoretis dan metodologis bagi pengembangan studi tentang manajemen risiko teknologi informasi menggunakan framework ISO 31000. Proses ini tidak hanya membantu peneliti memahami konteks dan perkembangan terkini dalam bidangnya tetapi juga memungkinkan mereka untuk mengidentifikasi kesenjangan pengetahuan serta merumuskan pertanyaan penelitian yang relevan. Dengan demikian, tinjauan pustaka menjadi komponen integral dalam menghasilkan penelitian yang berkualitas tinggi dan memberikan kontribusi berarti bagi perkembangan ilmu pengetahuan di bidang manajemen risiko TI.

IV. PEMBAHASAN DAN HASIL

4.1 Latar Belakang ISO 31000

Framework ISO 31000 adalah standar internasional yang memberikan pedoman untuk pengelolaan risiko yang efektif dan efisien di berbagai organisasi. Sejarah ISO 31000 dimulai pada tahun 2009 ketika International Organization for Standardization (ISO) merilis versi pertama dari standar ini. Sejak saat itu, framework ini telah mengalami beberapa revisi, dengan versi terbaru diterbitkan pada tahun 2018. Revisi ini bertujuan untuk memperbarui dan menyempurnakan panduan berdasarkan praktik terbaik dan pengalaman yang diperoleh dari penerapan di berbagai sektor [4].

Tujuan utama dari ISO 31000 adalah untuk menyediakan prinsip-prinsip dan kerangka kerja yang dapat digunakan oleh organisasi untuk mengelola risiko secara sistematis, terintegrasi, dan transparan. Standar ini tidak hanya berfokus pada risiko yang bersifat negatif, tetapi juga mencakup peluang yang dapat dimanfaatkan oleh organisasi untuk mencapai tujuan strategis mereka. ISO 31000 memberikan pendekatan holistik terhadap manajemen risiko, di mana semua jenis risiko baik yang bersifat finansial, operasional, reputasi, maupun strategis dapat diidentifikasi dan dikelola [7].

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

Gambar 1. Prinsip ISO 31000

Prinsip dasar dari ISO 31000 mencakup:

1. Integrasi: Manajemen risiko bukanlah aktivitas terpisah, melainkan bagian integral dari semua proses organisasi. Dalam hal ini, risiko harus dipertimbangkan dalam setiap aspek, mulai dari perencanaan strategis, pengambilan keputusan, hingga operasi sehari-hari. Misalnya, ketika organisasi merencanakan peluncuran produk baru, mereka harus mempertimbangkan risiko yang mungkin muncul, seperti gangguan rantai pasok atau reaksi negatif dari pasar. Integrasi manajemen risiko memastikan bahwa setiap keputusan mencakup analisis potensi ancaman dan peluang, sehingga organisasi dapat lebih siap menghadapi tantangan.
2. Terstruktur dan Komprehensif: Struktur dan Proses Organisasi harus memiliki struktur manajemen risiko yang jelas, termasuk peran dan tanggung jawab yang terdefinisi untuk setiap individu atau tim yang terlibat. Misalnya, divisi teknologi informasi bertanggung jawab mengidentifikasi risiko keamanan siber, sementara divisi keuangan fokus pada risiko pasar. Selain itu, organisasi perlu mengadopsi proses formal untuk mengidentifikasi, menilai, memantau, dan mengelola risiko. Struktur dan proses ini mencakup prosedur operasional, mekanisme pelaporan, serta alat untuk memantau efektivitas langkah-langkah mitigasi.
3. Disesuaikan: Manajemen risiko yang efektif melibatkan partisipasi dari semua pihak yang berkepentingan, baik internal maupun eksternal. Karyawan dapat memberikan masukan berdasarkan pengalaman operasional, sementara pelanggan dan pemasok mungkin memiliki wawasan tentang risiko yang tidak terlihat oleh manajemen internal. Dengan melibatkan berbagai pemangku kepentingan, organisasi dapat mengidentifikasi risiko dari berbagai sudut pandang, memastikan bahwa strategi

DOI: 10.52362/jisamar.v9i1.1690

mitigasi lebih komprehensif. Partisipasi aktif juga membangun rasa memiliki terhadap proses manajemen risiko, meningkatkan keberhasilan implementasinya.

4. Inklusif: Keputusan dalam manajemen risiko harus didasarkan pada data yang akurat dan relevan, bukan hanya asumsi atau intuisi. Hal ini melibatkan pengumpulan informasi yang valid, seperti catatan historis insiden, tren pasar, atau laporan audit, untuk mendukung proses pengambilan keputusan. Sebagai contoh, sebuah perusahaan yang menghadapi ancaman siber dapat menggunakan analisis data ancaman global untuk memprioritaskan investasi pada perlindungan tertentu. Pendekatan berbasis bukti memastikan keputusan lebih objektif dan terpercaya.
5. Dinamis: Setiap organisasi memiliki karakteristik unik yang memengaruhi pendekatan manajemen risikonya. Misalnya, organisasi besar dengan struktur kompleks membutuhkan pendekatan yang berbeda dibandingkan dengan usaha kecil. Selain itu, faktor eksternal seperti lingkungan hukum, budaya masyarakat, dan dinamika pasar juga harus diperhitungkan. Dengan memahami konteks ini, organisasi dapat merancang strategi manajemen risiko yang relevan dan efektif, sehingga lebih mampu menghadapi tantangan spesifik yang mereka hadapi.
6. Informasi terbaik yang tersedia: Transparansi adalah elemen penting dalam manajemen risiko. Organisasi harus berkomunikasi secara teratur dengan semua pemangku kepentingan mengenai risiko yang diidentifikasi, langkah-langkah mitigasi yang diambil, dan perkembangan terkini. Komunikasi yang efektif membangun kepercayaan antara tim internal dan eksternal, memastikan bahwa semua pihak memiliki pemahaman yang sama tentang prioritas risiko. Konsultasi dengan pihak-pihak terkait juga membantu organisasi untuk mendapatkan masukan berharga yang dapat memperkaya strategi manajemen risiko.
7. Faktor Manusia dan Budaya: Semua individu, dari manajemen puncak hingga karyawan di lapangan, perlu memiliki pemahaman yang sama tentang pentingnya manajemen risiko dan peran mereka dalam proses tersebut. Oleh karena itu, budaya organisasi yang mendukung kesadaran dan mitigasi risiko harus dibangun, di mana setiap individu merasa bertanggung jawab untuk mengidentifikasi dan mengelola risiko yang mungkin terjadi dalam pekerjaan mereka. Dengan demikian, budaya yang terbuka dan komunikatif, serta fokus pada pembelajaran dan peningkatan, akan memperkuat keseluruhan sistem manajemen risiko dalam organisasi.
8. Peningkatan Berkelanjutan: Manajemen risiko bukan proses yang statis; organisasi harus terus belajar dari pengalaman, umpan balik pemangku kepentingan, dan perubahan dalam lingkungan operasional. Contohnya, organisasi dapat memperbaiki sistem keamanan mereka berdasarkan analisis insiden sebelumnya atau menyesuaikan strategi mitigasi sesuai dengan perkembangan regulasi baru. Komitmen untuk peningkatan berkelanjutan memastikan bahwa proses manajemen risiko tetap relevan, responsif, dan selaras dengan kebutuhan organisasi yang terus berkembang [9].

Relevansi ISO 31000 dalam konteks teknologi informasi saat ini sangat signifikan. Di era digital yang ditandai oleh kemajuan pesat dalam teknologi seperti kecerdasan buatan (AI), Internet of Things (IoT), dan otomatisasi, organisasi menghadapi berbagai tantangan baru terkait keamanan siber, privasi data, dan kepatuhan terhadap regulasi yang terus berkembang. Dengan meningkatnya ketergantungan pada teknologi informasi, penting bagi organisasi untuk memiliki kerangka kerja manajemen risiko yang kuat untuk melindungi aset informasi mereka dan memastikan keberlanjutan operasional [10].

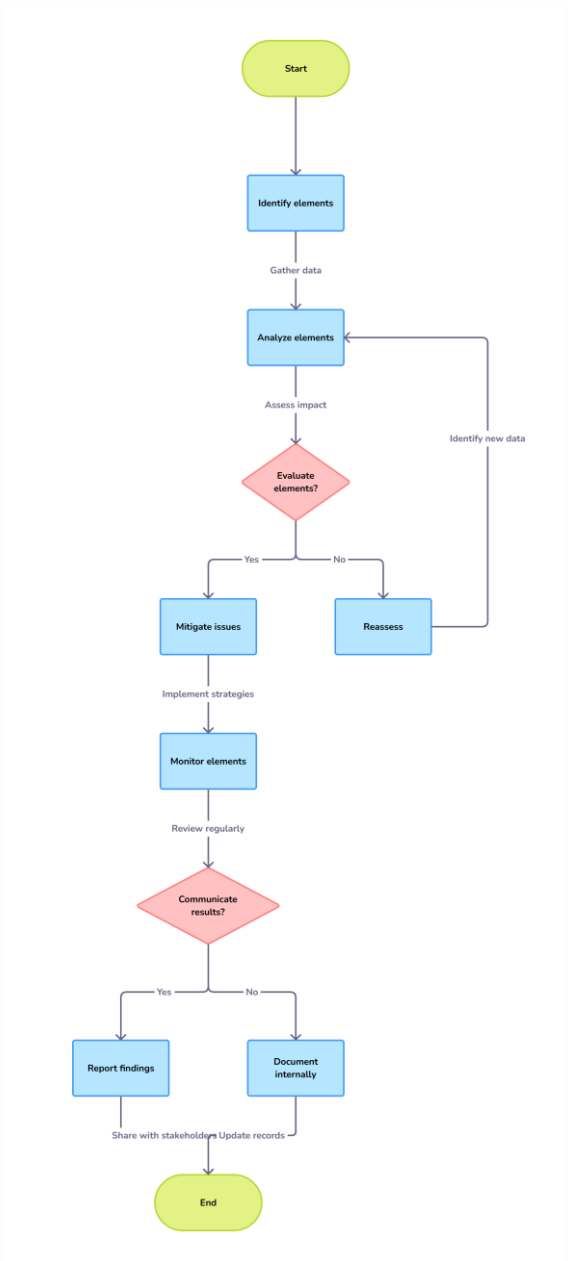
ISO 31000 memungkinkan organisasi untuk membangun kerangka kerja manajemen risiko yang lebih holistik, di mana setiap aspek dari operasi bisnis dipertimbangkan dalam konteks risiko. Hal ini sangat penting karena banyak organisasi masih menggunakan pendekatan reaktif dalam manajemen risiko TI, di mana risiko hanya ditangani setelah terjadinya insiden atau masalah [2].

Dengan demikian, penerapan framework ISO 31000 menjadi sangat relevan bagi organisasi yang ingin meningkatkan ketahanan mereka terhadap ancaman digital dan memanfaatkan peluang yang ada di pasar. Melalui pemahaman yang mendalam tentang prinsip-prinsip dasar dan tujuan dari ISO 31000, organisasi dapat mengembangkan strategi manajemen risiko yang lebih efektif dan terintegrasi dengan tujuan bisnis mereka secara keseluruhan.

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

4.2 Kerangka Kerja Manajemen Risiko



Gambar 2. Flowchart Proses Manajemen Risiko

Proses manajemen risiko menurut ISO 31000 terdiri dari beberapa langkah kunci yang saling terkait. Langkah-langkah ini dirancang untuk membantu organisasi mengidentifikasi, menganalisis, mengevaluasi, dan mengelola risiko secara sistematis:

1. **Identifikasi Risiko**: Tahap pertama dalam proses manajemen risiko adalah mengidentifikasi semua potensi risiko yang dapat memengaruhi pencapaian tujuan organisasi. Proses ini merupakan fondasi penting yang memastikan bahwa organisasi memiliki pemahaman menyeluruh tentang berbagai ancaman yang mungkin muncul. Teknik yang digunakan untuk identifikasi risiko meliputi brainstorming, yang melibatkan diskusi kelompok untuk mengumpulkan berbagai pandangan dan ide

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

terkait risiko potensial. Selain itu, wawancara dengan pemangku kepentingan internal dan eksternal dilakukan untuk memperoleh wawasan dari sudut pandang yang berbeda. Analisis dokumen, seperti data historis, laporan operasional, dan hasil audit, juga digunakan untuk mengidentifikasi pola risiko yang berulang. Pengamatan langsung terhadap operasi sehari-hari memberikan pandangan praktis tentang risiko yang sering tidak terlihat dalam analisis teoretis.

2. **Analisis Risiko**: Setelah risiko diidentifikasi, langkah berikutnya adalah menganalisis sifat dan karakteristik setiap risiko. Proses ini mencakup penilaian terhadap kemungkinan terjadinya risiko serta dampaknya jika terjadi. Untuk mempermudah analisis, matriks probabilitas-dampak sering digunakan. Matriks ini membantu mengklasifikasikan risiko berdasarkan tingkat urgensinya, sehingga organisasi dapat memprioritaskan perhatian pada risiko yang paling kritis. Misalnya, risiko dengan probabilitas tinggi dan dampak besar harus segera ditangani, sementara risiko dengan dampak kecil dapat dipantau lebih lanjut.
3. **Evaluasi Risiko**: Pada tahap evaluasi, organisasi menilai apakah risiko yang telah dianalisis dapat diterima atau perlu ditangani lebih lanjut. Keputusan ini dipandu oleh toleransi risiko organisasi, yaitu sejauh mana organisasi bersedia menerima risiko tertentu tanpa mengganggu operasi atau tujuan strategisnya. Evaluasi ini juga mempertimbangkan prioritas strategis organisasi, sehingga pengelolaan risiko selaras dengan visi dan misi yang telah ditetapkan.
4. **Pengelolaan Risiko (Mitigasi)**: Jika risiko memerlukan penanganan lebih lanjut, langkah berikutnya adalah merancang tindakan mitigasi untuk mengurangi atau menghilangkan dampak negatifnya. Tindakan mitigasi dapat berupa penerapan kontrol internal, seperti kebijakan keamanan yang lebih ketat atau prosedur operasional yang diperbarui. Pelatihan karyawan juga penting untuk memastikan bahwa staf memahami risiko yang relevan dan cara menghadapinya. Selain itu, pengembangan rencana darurat atau contingency plan memungkinkan organisasi merespons dengan cepat dan efektif jika risiko benar-benar terjadi.
5. **Pemantauan dan Tinjauan**: Manajemen risiko tidak berhenti setelah tindakan mitigasi diterapkan. Pemantauan berkelanjutan diperlukan untuk memastikan bahwa langkah-langkah yang diambil efektif dalam mengurangi risiko. Selain itu, pemantauan ini membantu mendeteksi munculnya risiko baru yang belum diidentifikasi sebelumnya. Tinjauan berkala terhadap seluruh proses manajemen risiko penting untuk menilai relevansi pendekatan yang digunakan serta untuk memperbarui strategi jika kondisi internal atau eksternal organisasi berubah.
6. **Komunikasi Hasil**: Langkah terakhir adalah memastikan bahwa semua hasil dari proses manajemen risiko dikomunikasikan kepada pemangku kepentingan terkait. Komunikasi ini penting agar semua pihak memahami risiko yang dihadapi organisasi, langkah-langkah mitigasi yang telah dilakukan, dan peran masing-masing dalam mendukung keberhasilan manajemen risiko. Komunikasi yang transparan juga membantu membangun kepercayaan dan kolaborasi antar departemen dalam menghadapi tantangan risiko [11].

Dengan mengikuti prinsip-prinsip dasar dan langkah-langkah dalam proses manajemen risiko menurut ISO 31000, organisasi dapat mengembangkan pendekatan yang lebih terstruktur dan sistematis dalam menghadapi tantangan-tantangan terkait teknologi informasi di era digital saat ini. Penerapan framework ini tidak hanya membantu dalam mengelola ancaman tetapi juga memungkinkan organisasi untuk memanfaatkan peluang dengan cara yang lebih aman dan terencana.

4.3 Studi Kasus Penerapan ISO 31000

4.3.1 Studi Kasus PT SAT

Penelitian oleh Atmojo dan Manuputty berfokus pada analisis manajemen risiko teknologi informasi dalam aplikasi AHO Office yang digunakan oleh PT SAT. Penelitian ini bertujuan untuk mengidentifikasi dan mendokumentasikan berbagai jenis risiko yang mungkin terjadi serta cara penanganannya dengan menggunakan framework ISO 31000. Dalam konteks ini, peneliti menerapkan metode kualitatif yang melibatkan wawancara dan observasi langsung untuk mendapatkan data yang akurat dan mendalam.

Proses penelitian dimulai dengan identifikasi risiko, di mana peneliti mengumpulkan informasi dari berbagai pemangku kepentingan di PT SAT, termasuk manajer TI dan staf operasional. Melalui wawancara, peneliti berhasil mengidentifikasi total 19 risiko yang berkaitan dengan penggunaan aplikasi AHO Office. Dari

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

hasil identifikasi tersebut, risiko-risiko ini kemudian dikategorikan berdasarkan tingkat keparahan dan kemungkinan terjadinya. Tiga dari risiko yang teridentifikasi dikategorikan sebagai risiko ekstrem, tujuh sebagai risiko tinggi, dan sisanya sebagai risiko sedang hingga rendah.

Risiko ekstrem yang ditemukan mencakup potensi kebocoran data sensitif dan serangan siber yang dapat mengakibatkan kerugian finansial yang signifikan bagi perusahaan. Risiko tinggi lainnya termasuk kegagalan sistem yang dapat menyebabkan gangguan operasional dan hilangnya produktivitas. Dengan mendokumentasikan berbagai jenis risiko ini, penelitian ini memberikan gambaran yang jelas tentang pentingnya manajemen risiko dalam konteks teknologi informasi.

Selanjutnya, penelitian ini tidak hanya fokus pada identifikasi risiko, tetapi juga mengeksplorasi langkah-langkah mitigasi yang dapat diambil untuk menangani risiko-risiko tersebut. Peneliti merekomendasikan beberapa strategi mitigasi berdasarkan temuan mereka, seperti peningkatan keamanan jaringan, penerapan protokol pemulihan bencana, serta pelatihan keamanan siber bagi karyawan. Rekomendasi ini bertujuan untuk membantu pemangku kebijakan dalam menyusun strategi mitigasi yang efektif dan proaktif.

Hasil dari penelitian ini menekankan pentingnya dokumentasi manajemen risiko sebagai alat bantu bagi organisasi dalam memahami profil risiko mereka. Dengan memiliki dokumentasi yang jelas tentang berbagai jenis risiko dan langkah-langkah mitigasi yang diambil, PT SAT dapat lebih siap menghadapi ancaman digital dan memastikan keberlanjutan operasional mereka.

4.3.2 Studi Kasus Universitas Sebelas April

Penelitian oleh Miftakhatun (2020) mengevaluasi penerapan framework ISO 31000 pada sistem Tracer Study di Universitas Sebelas April. Penelitian ini bertujuan untuk memahami dan meningkatkan proses manajemen risiko dalam konteks akademik, di mana pengelolaan data mahasiswa dan informasi terkait sangat penting. Dengan menggunakan metode kualitatif dan pendekatan deskriptif, peneliti berusaha untuk mendapatkan wawasan yang mendalam tentang proses bisnis dan struktur organisasi yang terlibat dalam sistem Tracer Study.

Proses penelitian dimulai dengan identifikasi risiko, yang dilakukan melalui observasi langsung terhadap operasional sistem serta wawancara dengan admin sistem Tracer Study. Melalui interaksi ini, peneliti dapat mengumpulkan informasi yang relevan mengenai potensi risiko yang mungkin dihadapi oleh sistem, termasuk risiko teknis, operasional, dan keamanan data. Hasil dari tahap ini menunjukkan bahwa terdapat berbagai risiko yang dapat mempengaruhi efektivitas sistem, mulai dari kesalahan dalam pengolahan data hingga ancaman keamanan siber.

Setelah identifikasi risiko, langkah berikutnya adalah analisis dan evaluasi risiko. Peneliti menganalisis setiap risiko berdasarkan frekuensi kejadian dan dampaknya terhadap operasional sistem. Proses ini memungkinkan peneliti untuk mengklasifikasikan risiko-risiko tersebut ke dalam kategori yang berbeda, sehingga memudahkan dalam merumuskan strategi mitigasi yang tepat. Penelitian ini menemukan bahwa beberapa risiko memiliki dampak signifikan terhadap kinerja sistem, sehingga memerlukan perhatian khusus dalam upaya mitigasi.

Berdasarkan hasil analisis, penelitian ini merekomendasikan penerapan strategi penanganan risiko yang tepat untuk meningkatkan keamanan dan kinerja operasional sistem Tracer Study. Salah satu strategi utama yang diusulkan adalah penerapan monitoring real-time untuk memantau aktivitas sistem secara terus-menerus. Dengan adanya pemantauan yang aktif, tim manajemen dapat dengan cepat mendeteksi dan merespons masalah yang muncul sebelum menjadi lebih serius. Selain itu, pelatihan pengguna juga menjadi salah satu rekomendasi penting. Pelatihan ini bertujuan untuk meningkatkan kesadaran pengguna tentang praktik terbaik dalam pengelolaan data serta cara-cara untuk menghindari potensi risiko.

Hasil penelitian ini menunjukkan bahwa penerapan strategi penanganan risiko yang tepat tidak hanya dapat meningkatkan keamanan data tetapi juga meningkatkan kinerja operasional sistem secara keseluruhan. Dengan adanya dokumentasi manajemen risiko yang jelas, pemangku kebijakan di Universitas Sebelas April dapat lebih efektif dalam menyusun strategi mitigasi yang sesuai dengan kebutuhan dan karakteristik spesifik dari sistem Tracer Study.

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

4.3.3 Studi Kasus PT Schlumberger Geophysics Nusantara

PT Schlumberger Geophysics Nusantara mengadopsi framework ISO 31000 untuk meningkatkan pengelolaan risiko dalam operasional teknologi informasi (TI) mereka. Penelitian yang dilakukan oleh Gina Patriani Manuputty et al. (2021) bertujuan untuk mengevaluasi efektivitas penerapan manajemen risiko berbasis ISO 31000 di perusahaan ini. Dalam penelitian tersebut, tim manajemen risiko di PT Schlumberger mengidentifikasi 14 jenis risiko yang berpotensi mengganggu operasi sehari-hari.

Proses penelitian dimulai dengan identifikasi risiko, di mana tim manajemen risiko melakukan analisis mendalam terhadap berbagai aspek operasional TI. Mereka menggunakan metode analisis deskriptif untuk mengumpulkan data dari 20 karyawan yang bekerja di Divisi TI. Melalui wawancara dan diskusi kelompok, peneliti berhasil mengidentifikasi berbagai risiko yang mencakup aspek teknis, operasional, dan keamanan data.

Setelah proses identifikasi, setiap risiko dievaluasi berdasarkan tingkat keparahan dan kemungkinan terjadinya. Peneliti menemukan bahwa dari 14 jenis risiko yang diidentifikasi, 11 risiko berada pada level tinggi, sementara 3 lainnya berada pada level moderat. Risiko-risiko tinggi tersebut termasuk ancaman serangan siber, kegagalan sistem TI, serta masalah terkait kepatuhan terhadap regulasi yang berlaku. Proses evaluasi ini penting untuk memahami dampak potensial dari masing-masing risiko terhadap operasional perusahaan.

Berdasarkan hasil evaluasi, tim manajemen risiko kemudian merumuskan strategi mitigasi yang komprehensif. Strategi ini mencakup peningkatan infrastruktur TI untuk memperkuat keamanan sistem, implementasi kontrol akses yang lebih ketat untuk melindungi data sensitif, serta pengembangan rencana tanggap darurat untuk menghadapi situasi krisis. Rencana tanggap darurat ini dirancang untuk memastikan bahwa perusahaan dapat dengan cepat merespons insiden yang mungkin terjadi dan meminimalkan dampak negatif terhadap operasi.

Hasil dari penerapan ISO 31000 di PT Schlumberger menunjukkan bahwa perusahaan mampu mengurangi waktu downtime sistem hingga 30% dalam enam bulan setelah implementasi. Ini adalah pencapaian signifikan yang menunjukkan efektivitas strategi mitigasi yang diterapkan. Selain itu, penelitian ini juga mencatat adanya peningkatan kesadaran karyawan mengenai pentingnya keamanan informasi. Kesadaran ini berdampak positif terhadap budaya organisasi dalam hal manajemen risiko, di mana karyawan menjadi lebih proaktif dalam mengidentifikasi dan melaporkan potensi risiko.

4.3.4 Studi Kasus PT XYZ Menggunakan Metode Failure Mode and Effects Analysis (FMEA)

Proses penelitian dimulai dengan identifikasi risiko, di mana tim manajemen risiko di PT XYZ melakukan analisis mendalam terhadap berbagai aspek operasional TI. Mereka menggunakan pendekatan kualitatif dengan wawancara dan diskusi kelompok untuk mengumpulkan informasi dari berbagai pemangku kepentingan, termasuk manajer TI, staf operasional, dan pengguna akhir. Melalui proses ini, tim berhasil mengidentifikasi sejumlah risiko yang dapat mempengaruhi kinerja sistem TI perusahaan.

Setelah identifikasi, setiap risiko dievaluasi dengan menggunakan metode FMEA untuk menilai tingkat keparahan dan kemungkinan terjadinya. Metode ini memberikan kerangka kerja yang sistematis untuk menganalisis potensi kegagalan dalam sistem dan dampaknya. Hasil dari evaluasi menunjukkan bahwa beberapa risiko memiliki dampak yang signifikan terhadap operasional perusahaan, sehingga memerlukan perhatian khusus dalam pengelolaan.

Penelitian ini menekankan pentingnya penggunaan COBIT 5 sebagai alat untuk memperkuat proses pengkajian risiko. Dengan mengintegrasikan COBIT 5 ke dalam framework ISO 31000, PT XYZ dapat memperoleh gambaran yang lebih jelas mengenai alur pengelolaan risiko yang terintegrasi. Hal ini memungkinkan organisasi untuk tidak hanya mengidentifikasi dan menganalisis risiko tetapi juga merumuskan strategi mitigasi yang lebih komprehensif.

Strategi mitigasi yang diusulkan mencakup peningkatan kontrol akses, penguatan infrastruktur TI, serta pengembangan rencana tanggap darurat untuk situasi krisis. Dengan langkah-langkah ini, PT XYZ berupaya untuk memastikan bahwa mereka dapat merespons dengan cepat terhadap insiden yang mungkin terjadi dan meminimalkan dampak negatif terhadap operasional.

Hasil dari penerapan kombinasi framework ini menunjukkan bahwa PT XYZ berhasil meningkatkan efektivitas manajemen risiko mereka secara keseluruhan. Penggunaan FMEA dalam konteks ISO 31000 dan COBIT 5 memberikan struktur yang lebih baik dalam pengelolaan risiko, serta meningkatkan kesadaran karyawan mengenai pentingnya keamanan informasi. Dengan adanya pendekatan yang terintegrasi ini,

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

perusahaan mampu mengurangi potensi kerugian akibat insiden TI dan meningkatkan kepercayaan pemangku kepentingan terhadap sistem manajemen risiko yang diterapkan.

4.3.5 Studi Kasus Tripio Purwokerto

Penelitian ini bertujuan untuk mengeksplorasi bagaimana kombinasi berbagai standar dapat memberikan pendekatan yang lebih komprehensif dalam pengelolaan risiko. Dengan menggunakan metode campuran, peneliti melakukan survei dan wawancara dengan staf TI serta manajemen untuk memahami bagaimana integrasi ini diterapkan dalam praktik.

Metode penelitian yang digunakan adalah metode campuran, yang menggabungkan survei dan wawancara. Peneliti melakukan survei untuk mengumpulkan data kuantitatif dari karyawan di berbagai level, termasuk manajer TI dan staf operasional, untuk mendapatkan gambaran umum tentang cara pengelolaan risiko saat ini. Selain itu, wawancara mendalam dilakukan dengan pemangku kepentingan kunci untuk memahami bagaimana integrasi antara ISO 31000 dan standar keamanan informasi lainnya diterapkan dalam praktik sehari-hari.

Hasil dari penelitian ini menunjukkan bahwa dengan menggabungkan ISO 31000 dengan standar keamanan informasi seperti NIST Cybersecurity Framework dan COBIT 5, Tripio Purwokerto dapat menciptakan kerangka kerja manajemen risiko yang lebih holistik. Integrasi ini memungkinkan perusahaan untuk tidak hanya fokus pada identifikasi dan mitigasi risiko, tetapi juga pada tata kelola dan kepatuhan terhadap regulasi yang berlaku. Dengan pendekatan ini, organisasi dapat lebih responsif terhadap perubahan lingkungan bisnis dan ancaman keamanan yang muncul.

Penelitian ini mencatat bahwa pendekatan terintegrasi ini membantu meningkatkan kesadaran akan keamanan informasi di seluruh organisasi. Karyawan menjadi lebih memahami pentingnya manajemen risiko dan peran mereka dalam menjaga keamanan sistem TI. Selain itu, kolaborasi antara berbagai departemen juga meningkat, karena semua pihak merasa memiliki tanggung jawab terhadap pengelolaan risiko.

Salah satu temuan kunci dari penelitian ini adalah bahwa penggunaan kombinasi beberapa framework tidak hanya memperkuat proses pengelolaan risiko tetapi juga meningkatkan efektivitas implementasi kebijakan keamanan informasi secara keseluruhan. Dengan adanya panduan yang jelas dari berbagai standar, organisasi dapat merumuskan strategi mitigasi yang lebih baik dan lebih terarah.

4.4 Analisis Perbandingan dengan Framework Lain

Dalam konteks manajemen risiko, terdapat beberapa framework yang relevan dan sering digunakan oleh organisasi untuk mengelola risiko, termasuk ISO 31000, COBIT 5, dan NIST Cybersecurity Framework. Masing-masing framework ini memiliki kelebihan dan kekurangan yang berbeda, serta situasi di mana satu framework mungkin lebih cocok daripada yang lain.

4.4.1 ISO 31000

ISO 31000 adalah standar internasional yang memberikan pedoman umum untuk pengelolaan risiko yang dapat diterapkan pada berbagai jenis organisasi, tanpa terbatas pada sektor tertentu. Standar ini bertujuan untuk membantu organisasi mengidentifikasi, menganalisis, mengevaluasi, dan mengelola risiko secara sistematis guna mendukung pencapaian tujuan strategis. Dengan pendekatan berbasis prinsip, ISO 31000 menekankan pentingnya integrasi manajemen risiko ke dalam semua aspek organisasi, termasuk strategi, operasi, dan pengambilan keputusan sehari-hari. Standar ini dirancang agar fleksibel dan dapat disesuaikan dengan berbagai ukuran dan kompleksitas organisasi.

Kerangka kerja ISO 31000 mencakup beberapa elemen utama, yaitu kepemimpinan dan komitmen, integrasi ke dalam proses organisasi, desain framework, implementasi, evaluasi, serta perbaikan berkelanjutan. Proses manajemen risikonya melibatkan komunikasi dan konsultasi, penentuan konteks, identifikasi risiko, analisis dan evaluasi risiko, penanganan risiko, serta pemantauan dan tinjauan berkala. Standar ini memberikan panduan yang terstruktur untuk memastikan pengelolaan risiko dilakukan secara efektif dan konsisten.

Salah satu kelebihan utama ISO 31000 adalah fleksibilitasnya, yang memungkinkan penerapan di berbagai sektor dan situasi. Selain itu, pendekatan holistiknya mendorong integrasi manajemen risiko ke dalam budaya organisasi, sehingga setiap keputusan dapat mempertimbangkan potensi risiko. Namun, implementasi standar ini sering kali menghadapi tantangan, seperti kurangnya panduan spesifik untuk situasi kompleks dan kebutuhan akan komitmen dari semua tingkatan organisasi. Integrasi ke dalam budaya organisasi juga

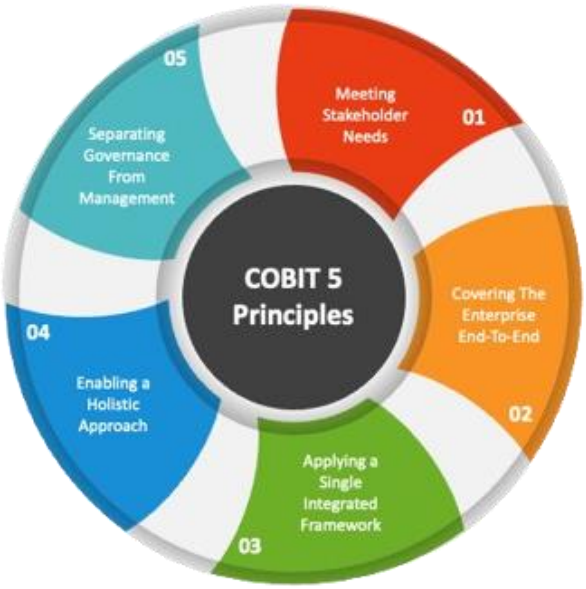
DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

memerlukan waktu dan upaya yang signifikan. Meskipun demikian, ISO 31000 tetap menjadi alat penting untuk meningkatkan pengambilan keputusan dan ketahanan organisasi terhadap ketidakpastian.

4.4.2 COBIT 5

Di sisi lain, COBIT (Control Objectives for Information and Related Technologies) adalah framework yang dirancang khusus untuk pengelolaan TI dan tata kelola informasi. Kelebihan dari COBIT adalah fokusnya pada tata kelola TI, memberikan kerangka kerja yang jelas untuk mengelola dan mengendalikan TI dalam konteks bisnis. COBIT juga mencakup praktik terbaik yang telah terbukti efektif dalam pengelolaan TI dan risiko terkait serta menyediakan alat penilaian yang kuat untuk mengevaluasi kinerja pengelolaan TI dan efektivitas kontrol. Namun, implementasi COBIT dapat menjadi kompleks dan memerlukan sumber daya yang signifikan untuk memahami dan menerapkan semua elemen framework. Selain itu, meskipun efektif untuk pengelolaan risiko TI, COBIT tidak mencakup aspek manajemen risiko secara keseluruhan di luar domain TI [12].



Gambar 3. COBIT 5 Principles

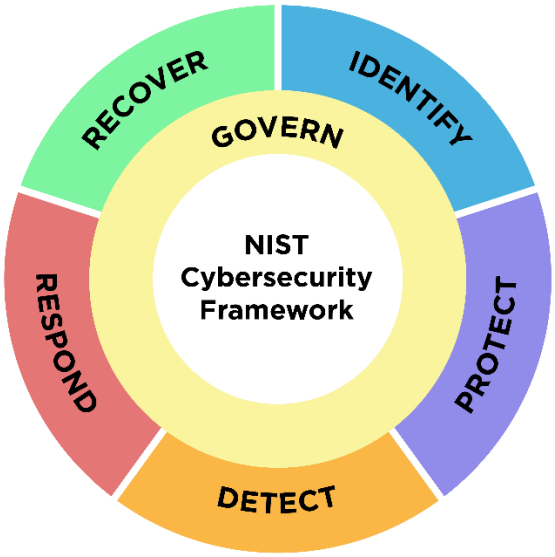
Framework ini dirancang untuk membantu organisasi menjembatani kesenjangan antara tujuan bisnis dan operasional TI, sehingga menciptakan sinergi antara keduanya. Dengan pendekatan yang komprehensif, COBIT mencakup berbagai aspek seperti pengelolaan sumber daya TI, pengukuran kinerja, dan mitigasi risiko TI. Namun, meskipun menawarkan banyak manfaat, implementasi COBIT sering kali memerlukan pemahaman mendalam terhadap framework serta alokasi sumber daya yang signifikan, baik dari segi waktu maupun tenaga kerja. Kompleksitas framework ini dapat menjadi tantangan, terutama bagi organisasi yang belum memiliki sistem tata kelola TI yang matang [13].

Selain itu, meskipun sangat efektif dalam pengelolaan risiko TI, COBIT memiliki cakupan yang terbatas pada domain TI dan tidak dirancang untuk mencakup manajemen risiko secara menyeluruh di luar lingkup teknologi informasi. Oleh karena itu, organisasi yang ingin mengelola risiko secara holistik perlu mengombinasikan COBIT dengan framework lain yang lebih luas, seperti ISO 31000. Meskipun demikian, COBIT tetap menjadi salah satu framework yang sangat berguna untuk memastikan pengelolaan dan pengendalian TI yang terarah, strategis, dan sesuai dengan kebutuhan bisnis [14].

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

4.4.3 NIST Cybersecurity Framework



Gambar 4. NIST Cybersecurity Framework

NIST Cybersecurity Framework adalah pedoman yang dikembangkan oleh National Institute of Standards and Technology (NIST) untuk membantu organisasi meningkatkan keamanan siber secara sistematis. Framework ini menggunakan pendekatan berbasis risiko, yang menekankan pentingnya memahami risiko siber yang spesifik bagi setiap organisasi. Pendekatan ini memungkinkan organisasi untuk mengidentifikasi ancaman potensial, menilai kerentanannya, dan mengambil tindakan yang tepat untuk melindungi aset digitalnya. Salah satu keunggulan utama dari NIST Cybersecurity Framework adalah fleksibilitasnya, yang memungkinkan organisasi menyesuaikan pendekatan keamanan siber mereka berdasarkan kebutuhan, ukuran, dan kompleksitas operasional. Selain itu, framework ini dirancang untuk membantu organisasi memenuhi persyaratan kepatuhan terhadap regulasi keamanan siber yang berlaku [15].

Berdasarkan gambar 4 Framework ini terdiri dari lima fungsi inti yakni **Identify, Protect, Detect, Respond, dan Recover** yang mencakup berbagai aspek keamanan siber, mulai dari identifikasi aset hingga pemulihan setelah insiden. Fungsi-fungsi ini memberikan struktur yang jelas untuk membantu organisasi mengelola risiko siber secara proaktif. Dengan sifatnya yang modular, framework ini dapat diterapkan oleh berbagai jenis organisasi, baik yang memiliki keahlian keamanan siber yang mendalam maupun yang baru memulai upaya perlindungan siber [16].

Namun, framework ini lebih cocok digunakan oleh organisasi yang beroperasi dalam lingkungan dengan ancaman siber yang tinggi atau yang diwajibkan mematuhi regulasi keamanan tertentu. Meskipun memberikan panduan yang kuat untuk keamanan informasi, NIST Cybersecurity Framework tidak mencakup aspek manajemen risiko secara menyeluruh di luar domain keamanan siber. Oleh karena itu, organisasi yang ingin mengelola risiko bisnis secara holistik mungkin perlu mengintegrasikan framework ini dengan pedoman lain, seperti ISO 31000. Kendati demikian, NIST Cybersecurity Framework tetap menjadi alat yang sangat efektif untuk memperkuat postur keamanan siber organisasi dalam menghadapi lanskap ancaman yang terus berkembang.

Pemilihan framework manajemen risiko yang tepat sangat bergantung pada konteks spesifik organisasi. ISO 31000 lebih cocok untuk organisasi yang mencari pendekatan holistik dalam pengelolaan risiko di seluruh aspek operasional mereka. Organisasi dengan budaya kolaboratif yang ingin mengintegrasikan manajemen risiko ke dalam strategi bisnis mereka akan mendapatkan manfaat besar dari penerapan ISO 31000. Sebaliknya, COBIT 5 lebih ideal bagi organisasi yang berfokus pada tata kelola TI dan ingin memastikan bahwa pengelolaan TI mereka mendukung tujuan bisnis secara efektif. Perusahaan-perusahaan besar dengan infrastruktur TI kompleks

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

mungkin menemukan COBIT sebagai alat yang sangat berharga untuk mengelola risiko terkait teknologi informasi. Di sisi lain, NIST Cybersecurity Framework paling cocok untuk organisasi di sektor keuangan atau kesehatan, di mana data sensitif dikelola dan ancaman siber menjadi perhatian utama.

Dengan demikian, analisis perbandingan ini menunjukkan bahwa setiap framework ISO 31000, COBIT 5, dan NIST Cybersecurity Framework memiliki kelebihan dan kekurangan masing-masing serta konteks penerapan yang berbeda. Pemilihan framework harus didasarkan pada kebutuhan spesifik organisasi, tujuan strategis, serta lingkungan operasionalnya. Dengan memahami karakteristik masing-masing framework, organisasi dapat membuat keputusan yang lebih baik tentang pendekatan manajemen risiko mana yang paling sesuai untuk meningkatkan ketahanan mereka terhadap ancaman digital saat ini.

4.5 Tantangan dan Solusi dalam Implementasi

Implementasi framework ISO 31000 dalam manajemen risiko teknologi informasi (TI) sering kali dihadapkan pada berbagai tantangan yang dapat menghambat efektivitasnya. Tantangan-tantangan ini dapat berasal dari berbagai aspek, termasuk budaya organisasi, sumber daya, dan pengetahuan tentang proses manajemen risiko.

Salah satu tantangan utama adalah **resistensi terhadap perubahan budaya organisasi**. Banyak organisasi memiliki cara kerja dan kebiasaan yang telah terbangun selama bertahun-tahun, sehingga sulit untuk mengubah pola pikir dan perilaku karyawan terkait manajemen risiko. Resistensi ini sering kali muncul karena ketidakpahaman tentang pentingnya manajemen risiko atau ketakutan akan perubahan yang dapat mempengaruhi pekerjaan sehari-hari mereka. Untuk mengatasi tantangan ini, penting bagi organisasi untuk melakukan sosialisasi yang efektif mengenai manfaat penerapan ISO 31000 dan bagaimana hal tersebut dapat meningkatkan kinerja serta keamanan organisasi. Pelatihan yang berkelanjutan dan keterlibatan karyawan dalam proses pengambilan keputusan terkait manajemen risiko juga dapat membantu mengurangi resistensi [17].

Tantangan lain yang signifikan adalah **kurangnya sumber daya**, baik dalam hal finansial maupun manusia. Banyak organisasi, terutama yang lebih kecil, mungkin tidak memiliki anggaran yang cukup untuk melaksanakan program pelatihan atau untuk mengimplementasikan teknologi yang diperlukan untuk mendukung manajemen risiko. Selain itu, kurangnya personel yang terlatih dalam manajemen risiko TI dapat menyebabkan kesulitan dalam menerapkan framework ISO 31000 secara efektif. Untuk mengatasi masalah ini, organisasi perlu mengevaluasi kembali prioritas mereka dan mencari cara untuk mengalokasikan sumber daya dengan lebih efisien. Misalnya, mereka dapat memanfaatkan pelatihan online atau program mentorship yang lebih terjangkau untuk meningkatkan pengetahuan staf tanpa harus mengeluarkan biaya besar [18].

Selanjutnya, **ketidakpahaman tentang proses manajemen risiko** juga menjadi tantangan utama bagi banyak organisasi. Tanpa pemahaman yang jelas tentang langkah-langkah dalam framework ISO 31000, implementasi dapat menjadi tidak efektif dan tidak terarah. Oleh karena itu, penting bagi organisasi untuk menyediakan pelatihan yang komprehensif mengenai proses manajemen risiko, termasuk identifikasi, analisis, evaluasi, dan mitigasi risiko. Dengan memberikan panduan praktis dan contoh nyata dari penerapan ISO 31000, karyawan akan lebih siap untuk menerapkan prinsip-prinsip tersebut dalam pekerjaan mereka sehari-hari [19].

Selain itu, tantangan terkait **integrasi manajemen risiko ke dalam strategi bisnis** juga sering dihadapi oleh organisasi. Banyak perusahaan masih memandang manajemen risiko sebagai fungsi pendukung yang terpisah dari keputusan strategis utama. Hal ini menciptakan kesenjangan antara kebijakan manajemen risiko dan praktik operasional sehari-hari. Untuk mengatasi hal ini, penting bagi manajemen puncak untuk menunjukkan komitmen terhadap integrasi manajemen risiko dengan memasukkan elemen-elemen risiko dalam perencanaan strategis dan pengambilan keputusan. Dengan demikian, seluruh organisasi akan memahami bahwa manajemen risiko adalah bagian integral dari pencapaian tujuan bisnis [20].

Terakhir, **kurangnya sistem pemantauan dan tinjauan** juga menjadi kendala dalam implementasi ISO 31000. Tanpa pemantauan berkelanjutan terhadap efektivitas tindakan mitigasi yang diambil, organisasi mungkin tidak menyadari adanya perubahan dalam profil risiko mereka atau keberhasilan strategi yang diterapkan. Oleh karena itu, organisasi perlu membangun sistem pemantauan yang kuat untuk mengevaluasi hasil dari langkah-langkah mitigasi yang telah diterapkan serta melakukan tinjauan berkala terhadap proses manajemen risiko secara keseluruhan [21].

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

4.6 Peran Teknologi dalam Manajemen Risiko

Dalam era digital saat ini, teknologi informasi modern memainkan peran yang sangat penting dalam mendukung penerapan framework ISO 31000 dalam manajemen risiko. Berbagai teknologi, seperti big data analytics, machine learning, dan artificial intelligence (AI), dapat meningkatkan efisiensi dalam identifikasi dan penilaian risiko, serta membantu organisasi dalam pengambilan keputusan berbasis data.

Big data analytics memungkinkan organisasi untuk mengumpulkan dan menganalisis volume data yang sangat besar dari berbagai sumber. Dengan menggunakan teknik analisis yang canggih, organisasi dapat mengidentifikasi pola dan tren yang mungkin tidak terlihat dengan metode tradisional. Misalnya, dalam konteks manajemen risiko TI, big data analytics dapat digunakan untuk menganalisis data historis tentang insiden keamanan siber, sehingga membantu organisasi memahami faktor-faktor yang berkontribusi terhadap risiko tersebut. Dengan informasi ini, organisasi dapat mengambil langkah-langkah proaktif untuk mengurangi kemungkinan terjadinya insiden serupa di masa depan [22].

Machine learning juga berperan penting dalam meningkatkan manajemen risiko. Algoritma machine learning dapat digunakan untuk memprediksi risiko berdasarkan data historis dan pola perilaku. Misalnya, sistem dapat dilatih untuk mengenali tanda-tanda awal dari potensi serangan siber atau pelanggaran keamanan lainnya. Dengan kemampuan untuk belajar dari data baru secara terus-menerus, machine learning memungkinkan organisasi untuk menyesuaikan strategi mitigasi mereka secara dinamis dan responsif terhadap ancaman yang berkembang [23].

Selain itu, penggunaan artificial intelligence (AI) dalam manajemen risiko memberikan kemampuan untuk otomatisasi proses identifikasi dan penilaian risiko. AI dapat memproses informasi dengan kecepatan yang jauh lebih tinggi dibandingkan manusia, sehingga mempercepat waktu respons terhadap ancaman. Misalnya, sistem berbasis AI dapat secara otomatis memantau aktivitas jaringan dan mendeteksi anomali yang mungkin menunjukkan adanya serangan siber. Dengan demikian, AI tidak hanya membantu dalam mengidentifikasi risiko lebih cepat tetapi juga memungkinkan tim TI untuk fokus pada tugas-tugas strategis lainnya [24].

Teknologi juga mendukung pengambilan keputusan berbasis data dalam manajemen risiko. Dengan menyediakan analisis yang mendalam dan visualisasi data yang jelas, teknologi memungkinkan pemangku kepentingan untuk memahami situasi risiko dengan lebih baik. Penggunaan dashboard interaktif dan alat visualisasi lainnya dapat membantu manajemen dalam mengevaluasi profil risiko secara real-time dan membuat keputusan yang lebih informasi tentang langkah-langkah mitigasi yang perlu diambil.

Namun, meskipun teknologi menawarkan banyak manfaat dalam manajemen risiko, organisasi harus tetap waspada terhadap tantangan yang mungkin muncul. Kebergantungan pada teknologi juga membawa risiko baru, seperti kerentanan terhadap serangan siber yang ditargetkan pada sistem TI itu sendiri. Oleh karena itu, penting bagi organisasi untuk tidak hanya mengandalkan teknologi tetapi juga memastikan bahwa mereka memiliki kebijakan dan prosedur manajemen risiko yang kuat untuk melindungi aset informasi mereka.

4.7 Implikasi Kebijakan dan Rekomendasi untuk Praktik Terbaik

Integrasi manajemen risiko teknologi informasi (TI) dengan strategi bisnis secara keseluruhan adalah langkah krusial bagi organisasi yang ingin meningkatkan ketahanan mereka terhadap ancaman digital. Untuk mencapai hal ini, organisasi perlu mengembangkan kebijakan yang mendukung penerapan framework ISO 31000 secara efektif. Rekomendasi kebijakan berikut dapat membantu organisasi dalam mengintegrasikan manajemen risiko TI ke dalam strategi bisnis mereka.

Pertama, organisasi harus menetapkan **komitmen dari tingkat manajemen puncak** untuk mendukung manajemen risiko sebagai bagian integral dari strategi bisnis. Manajemen puncak harus secara aktif terlibat dalam proses pengelolaan risiko, mempromosikan kesadaran risiko di seluruh organisasi, dan memastikan bahwa semua karyawan memahami pentingnya manajemen risiko. Dengan dukungan yang kuat dari manajemen, budaya organisasi yang proaktif terhadap risiko dapat dibangun, sehingga setiap individu merasa bertanggung jawab untuk mengidentifikasi dan mengelola risiko dalam pekerjaan mereka f.

Kedua, penting bagi organisasi untuk **mengembangkan kebijakan manajemen risiko yang jelas dan terstruktur**. Kebijakan ini harus mencakup tujuan dan prinsip-prinsip manajemen risiko, serta prosedur yang sistematis untuk identifikasi, analisis, evaluasi, dan mitigasi risiko. Kebijakan ini juga perlu disosialisasikan kepada seluruh anggota organisasi agar semua pihak memahami peran mereka dalam pengelolaan risiko. Selain

DOI: 10.52362/jisamar.v9i1.1690

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 9 No.2 (February 2025)

itu, kebijakan harus diperbarui secara berkala untuk mencerminkan perubahan dalam lingkungan bisnis dan teknologi.

Ketiga, organisasi perlu **memanfaatkan teknologi informasi modern** untuk mendukung proses manajemen risiko. Penggunaan big data analytics, machine learning, dan artificial intelligence dapat meningkatkan efisiensi dalam identifikasi dan penilaian risiko. Dengan memanfaatkan teknologi ini, organisasi dapat menganalisis data dalam jumlah besar untuk mengidentifikasi pola dan tren yang relevan dengan risiko TI. Selain itu, teknologi dapat membantu dalam pengambilan keputusan berbasis data, sehingga memungkinkan organisasi untuk merespons ancaman dengan lebih cepat dan efektif.

Keempat, penting bagi organisasi untuk melakukan **pelatihan dan pengembangan berkelanjutan** bagi karyawan terkait manajemen risiko TI. Pelatihan ini harus mencakup pemahaman tentang framework ISO 31000 serta keterampilan praktis dalam mengidentifikasi dan mengelola risiko. Dengan meningkatkan pengetahuan dan keterampilan karyawan, organisasi akan memiliki sumber daya manusia yang lebih siap menghadapi tantangan terkait keamanan siber dan risiko TI lainnya.

Selanjutnya, organisasi harus membangun **mekanisme pemantauan dan tinjauan** yang efektif untuk mengevaluasi efektivitas strategi manajemen risiko yang diterapkan. Pemantauan berkelanjutan terhadap profil risiko serta tinjauan berkala terhadap kebijakan dan prosedur manajemen risiko akan membantu organisasi untuk tetap responsif terhadap perubahan kondisi internal dan eksternal. Melalui proses ini, organisasi dapat memastikan bahwa langkah-langkah mitigasi yang diambil tetap relevan dan efektif.

Terakhir, penting bagi organisasi untuk melihat manajemen risiko bukan hanya sebagai kewajiban tetapi juga sebagai **kesempatan untuk menciptakan nilai tambah**. Dengan mengintegrasikan manajemen risiko ke dalam strategi bisnis, organisasi dapat mengidentifikasi peluang baru yang mungkin muncul dari pengelolaan risiko yang baik. Misalnya, dengan memahami potensi ancaman terhadap data pelanggan, organisasi dapat mengambil langkah-langkah proaktif untuk melindungi informasi tersebut, sehingga meningkatkan kepercayaan pelanggan dan reputasi perusahaan.

V. KESIMPULAN

Dalam penelitian ini, telah dibahas penerapan framework ISO 31000 dalam manajemen risiko teknologi informasi (TI) dan bagaimana pendekatan ini dapat membantu organisasi dalam mengidentifikasi, menganalisis, dan mengelola risiko secara sistematis. Temuan utama menunjukkan bahwa penerapan ISO 31000 tidak hanya meningkatkan ketahanan organisasi terhadap ancaman digital, tetapi juga memungkinkan integrasi manajemen risiko ke dalam strategi bisnis secara keseluruhan. Dengan pendekatan yang holistik dan terstruktur, organisasi dapat lebih siap menghadapi tantangan yang muncul di era digital yang terus berkembang.

Dari analisis yang dilakukan, beberapa tantangan signifikan dalam penerapan ISO 31000 telah diidentifikasi, termasuk resistensi terhadap perubahan budaya organisasi, kurangnya sumber daya, ketidakpahaman tentang proses manajemen risiko, dan tantangan dalam integrasi manajemen risiko ke dalam strategi bisnis. Namun, solusi praktis telah diusulkan untuk mengatasi tantangan-tantangan ini, seperti peningkatan pelatihan dan sosialisasi mengenai pentingnya manajemen risiko, pengembangan kebijakan yang jelas, serta pemanfaatan teknologi modern untuk mendukung proses manajemen risiko.

Meskipun penelitian ini memberikan wawasan yang berharga tentang penerapan ISO 31000 dalam konteks TI, masih terdapat area-area yang memerlukan eksplorasi lebih lanjut. Salah satu area yang perlu diteliti lebih dalam adalah **pengaruh budaya organisasi terhadap keberhasilan implementasi manajemen risiko**. Penelitian lebih lanjut dapat mengeksplorasi bagaimana faktor-faktor budaya mempengaruhi sikap karyawan terhadap manajemen risiko dan bagaimana organisasi dapat membangun budaya yang mendukung pengelolaan risiko secara proaktif.

Selain itu, **studi longitudinal** diperlukan untuk mengevaluasi efektivitas jangka panjang dari penerapan ISO 31000 di berbagai sektor industri. Penelitian ini dapat memberikan pemahaman yang lebih mendalam tentang bagaimana organisasi menyesuaikan strategi manajemen risiko mereka seiring dengan perkembangan teknologi dan perubahan lingkungan bisnis.

Akhirnya, dengan pesatnya kemajuan teknologi seperti big data analytics dan artificial intelligence, penting untuk menyelidiki bagaimana teknologi ini dapat diintegrasikan lebih lanjut ke dalam framework ISO 31000. Penelitian di masa depan dapat fokus pada pengembangan alat dan metodologi baru yang memanfaatkan teknologi canggih untuk meningkatkan efisiensi dan efektivitas dalam identifikasi dan penilaian risiko.

DOI: 10.52362/jisamar.v9i1.1690

REFERENSI

[1] S. D. Kuncoro, R. A. Ghaisan, M. U. Zaky, and A. Wulansari, "Manajemen Risiko pada Teknologi Informasi : Studi Kasus pada Perusahaan Jasa," vol. 1, pp. 313–323, 2023.

[2] A. Kurniati, L. E. Nugroho, and M. N. Rizal, "Manajemen Risiko Teknologi Informasi pada e-Government : Ulasan Literatur Sistematis Information Technology Risk Management on e-Government : Systematic Literature Review," vol. 22, no. 2, pp. 207–222, 2020.

[3] S. A. Atmojo, A. D. Manuputty, J. D. No, K. Sidorejo, K. Salatiga, and J. Tengah, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office," vol. 7, no. 3, pp. 546–558, 2020.

[4] A. A. Herlambang, A. A. Gani, and D. D. Alvianto, "Pendekatan ISO 31000 : 2018 dalam Manajemen Risiko Teknologi Informasi pada Tracer Study Universitas Sebelas April ISO 31000 : 2018 Approach to Information Technology Risk Management in the Tracer Study at Universitas Sebelas April," no. September, pp. 5651–5660, 2024.

[5] G. P. Manuputty, A. A. Azis, and N. A. N. Pratami, "ANALISIS MANAJEMEN RISIKO BERBASIS ISO 31000 PADA ASPEK OPERASIONAL TEKNOLOGI INFORMASI PT. SCHLUMBERGER GEOPHYSICS NUSANTARA".

[6] H. I. Pribadi, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000 : 2018 Dengan FMEA (Studi Kasus PT Pertamina)," vol. 01, pp. 28–35, 2020.

[7] 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 Information System Risk Management Using ISO 31000 and ISO / EIC 27001 Control Standards in Tripio Purwokerto," vol. 20, no. 2, pp. 389–396, 2021, doi: 10.30812/matrik.v20i2.1093.

[8] S. Kraus and S. Dasí-rodríguez, "The art of crafting a systematic literature review in entrepreneurship research," 2020.

[9] Y. Erlika, M. I. Herdiansyah, and A. H. Mirza, "Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000," vol. 11, no. 01, 2020.

[10] A. Syaputra, I. Teknologi, P. Alam, and K. P. Alam, "Penilaian IT Governance dalam Manajemen Risiko IT Menggunakan Metode Quantitative dan Qualitative Risk Analysis Assessment of IT Governance in IT Risk Management Using Quantitative Methods and Qualitative Risk Analysis," vol. 12, no. April, pp. 63–73, 2022.

[11] D. Y. Andika, A. F. Wijaya, F. T. Informasi, U. Kristen, S. Wacana, and T. L. Timur, "MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK ISO 31000:2018 PADA PT. TRUST LERINVITAL TIMUR Diky," vol. 5, no. 2, pp. 111–118, 2022.

[12] S. Kasus, M. Kamal, and S. Firdaus, "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework Cobit 5," vol. 3, no. 2, pp. 3–8, 2020.

[13] M. Andre, G. Wattimena, and A. R. Tanaamah, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 Pada TSI / Teknologi dan Sistem Informasi Perpustakaan UKSW," vol. 3, no. 3, pp. 483–498, 2021.

[14] N. Made *et al.*, "Analisa Pengaruh Manajemen Risiko Teknologi Informasi Framework COBIT 5 Pada

DOI: 10.52362/jisamar.v9i1.1690

Karyawan (Studi Kasus : PT . Bukit Makmur Mandiri Utama Balikpapan) Penelitian ini bertujuan untuk mengetahui dan menganalisis bagaimana pengaruh software SPSS . Hasil olah data dapat dijadikan bahan evaluasi dalam menjalankan This study aims to determine and analyze how the influence of IT Risk Management on the employees of PT . Bukit Makmur Mandiri Utama . The business world in the field of information systems so that makes PT . BUMA as a," vol. 6, no. 1, pp. 1–9.

[15] Megawati and S. Rosnawati, "PENILAIAN RISIKO JARINGAN KOMPUTER MENGGUNAKAN FRAMEWORK NIST SP 800-30 REVISI 1 PADA SMK MUHMMADIYAH 2," vol. 8, no. 2, pp. 189–195, 2022.

[16] C. R. Simanjuntak, S. A. Pratama, and G. Barovih, "Remanajemen Jaringan Menggunakan Framework NIST Pada Perpustakaan Daerah Provinsi Sumatera Selatan," vol. 4, no. 1, pp. 152–163, 2023.

[17] N. Azizi and B. Rowlands, "IT Risk Management Implementation as Socio-Technical Change : A Process Approach," pp. 505–515, 2019.

[18] R. Marvin and H. Stein, *Risk Assessment Theory, Methods, and Applications*.

[19] A. N. Rahmatika, M. F. Apriyadi, and M. A. Kahfi, "Jurnal Manajemen dan Teknologi Informasi (JMTI) ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA SISTEM INFORMASI AKADEMIK (SIAK) UNIVERSITAS MUHAMMADIYAH SUKABUMI (UMM) MENGGUNAKAN ISO 31000," vol. 14, no. 1, pp. 48–57, 2024.

[20] I. Akkiyat and N. Souissi, "Modelling Risk Management Process According to ISO Standard," vol. 3878, no. 2, pp. 5830–5835, 2019, doi: 10.35940/ijrte.B3751.078219.

[21] P. T. Xyz and M. Framework, "INFORMASI DAN PEMETAAN MATURITY LEVEL PADA," pp. 43–54.

[22] S. D. Legawa and P. S. Informatika, "ENTERPRISE RISK MANAGEMENT PADA CLOUD COMPUTING," 2017.

[23] M. S. Irwanto, F. A. Bachtiar, and N. Yudistira, "COMPUTED INPUT WEIGHT EXTREME LEARNING MACHINE DENGAN REDUKSI DIMENSI PRINCIPAL COMPONENT ANALYSIS CLASSIFICATION OF HUMAN ACTIVITY USING COMPUTED INPUT WEIGHT EXTREME LEARNING MACHINE ALGORITHM WITH PRINCIPAL COMPONENT," vol. 9, no. 6, pp. 1195–1202, 2022, doi: 10.25126/jtiik.202295504.

[24] M. S. Y. Lubis, "MPLEMENTASI ARTIFICIAL INTELLIGENCE PADA SYSTEMMANUFAKTUR TERPADU," pp. 1–7.

DOI: 10.52362/jisamar.v9i1.1690