Madani: Jurnal Ilmiah Multidisiplin
Volume 4, Nomor 8, September, P. 177-182
E-ISSN: 2986-6340
Licenced by CC BY-SA 4.0
DOI: https://doi.org/10.5281/zenodo.22870979

Konsep Dasar Manajemen Risiko Dalam Pengelolaan Organisasi

Basic Concepts of Risk Management in Organizational Management

Abdurrahman Arrasidi[1], Akbar Lubis[2], Al Amin Lubis[3], Amelia Marcella[4], Muhammad Ryan Huda Manurung[5]

[1-5]Manajemen, Universitas Muslim Nusantara Al Washliyah, Indonesia
Email korespondensi: ameliagamie@gmail.com

Abstrak

Manajemen risiko merupakan bagian penting dari proses pengambilan keputusan karena organisasi beroperasi dalam lingkungan yang mengandung ketidakpastian. Artikel ini bertujuan menjelaskan konsep dasar manajemen risiko, tahapan prosesnya, jenis risiko, prinsip pengelolaan, serta keterkaitannya dengan tata kelola dan kinerja organisasi. Metode yang digunakan adalah kajian literatur konseptual dengan menelaah ISO 31000:2018, COSO Enterprise Risk Management, prinsip Basel Committee, serta literatur akademik mengenai risk assessment dan enterprise risk management. Hasil kajian menunjukkan bahwa manajemen risiko tidak seharusnya diposisikan hanya sebagai aktivitas kepatuhan atau fungsi pengendalian setelah risiko terjadi. Manajemen risiko perlu diintegrasikan dengan penetapan tujuan, strategi, proses bisnis, pengalokasian sumber daya, komunikasi, dan evaluasi kinerja. Proses dasarnya mencakup penetapan konteks, identifikasi, analisis, evaluasi, perlakuan, pemantauan, serta komunikasi risiko. Efektivitasnya ditentukan oleh kualitas informasi, budaya risiko, kepemimpinan, kejelasan risk appetite, dan mekanisme monitoring. Dalam lingkungan bisnis yang semakin digital dan kompleks, pendekatan risiko juga perlu mempertimbangkan risiko teknologi, siber, pihak ketiga, perubahan regulasi, reputasi, serta risiko strategis. Dengan demikian, konsep dasar manajemen risiko dapat menjadi fondasi bagi organisasi untuk mengurangi potensi kerugian sekaligus meningkatkan kemampuan beradaptasi dan mempertahankan nilai jangka panjang.
Kata kunci: *manajemen risiko; enterprise risk management; ISO 31000; tata kelola; risiko digital*

Abstract

Risk management is an essential component of the decision-making process because organizations operate in environments characterized by uncertainty. This article aims to explain the basic concepts of risk management, its process stages, types of risk, management principles, and its relationship with organizational governance and performance. The method employed is a conceptual literature review examining ISO 31000:2018, the COSO Enterprise Risk Management framework, the principles of the Basel Committee, and academic literature on risk assessment and enterprise risk management. The findings indicate that risk management should not be positioned merely as a compliance activity or a control function performed after risks occur. Instead, risk management should be integrated with goal setting, strategy, business processes, resource allocation, communication, and performance evaluation. The fundamental process encompasses establishing the context, risk identification, risk analysis, risk evaluation, risk treatment, risk monitoring, and risk communication. Its effectiveness is determined by the quality of information, risk culture, leadership, clarity of risk appetite, and monitoring mechanisms. In an increasingly digital and complex business environment, risk management approaches should also consider technology, cybersecurity, third-party, regulatory change, reputational, and strategic risks. Thus, the basic concepts of risk management can serve as a foundation for organizations to reduce potential losses while enhancing their ability to adapt and sustain long-term value.
Keywords: *risk management; enterprise risk management; ISO 31000; governance; digital risk*

Article Info
Received date: 20 August 2026 Revised date: 28 August 2026 Accepted date: 17 September 2026

PENDAHULUAN

Organisasi pada dasarnya tidak pernah beroperasi dalam kondisi yang sepenuhnya pasti. Setiap keputusan investasi, ekspansi, penggunaan teknologi, pengelolaan sumber daya manusia, maupun pelayanan kepada pelanggan mengandung kemungkinan munculnya hasil yang berbeda dari yang

direncanakan. Ketidakpastian tersebut dapat menghasilkan kerugian, tetapi dalam kondisi tertentu juga dapat membuka peluang. Karena itu, manajemen risiko tidak tepat dipahami hanya sebagai kegiatan untuk menghindari risiko. Perspektif yang lebih luas menempatkan manajemen risiko sebagai proses untuk memahami ketidakpastian, menentukan respons yang sesuai, dan menjaga agar keputusan organisasi tetap sejalan dengan tujuan yang telah ditetapkan (Aven, 2016).

ISO 31000:2018 memberikan kerangka generik yang dapat diterapkan pada berbagai jenis organisasi dan aktivitas. Standar tersebut menekankan bahwa manajemen risiko perlu diintegrasikan ke dalam tata kelola, strategi, perencanaan, pelaporan, kebijakan, nilai, dan budaya organisasi. ISO juga menekankan penciptaan dan perlindungan nilai, keterlibatan pemangku kepentingan, penyesuaian dengan konteks organisasi, serta perbaikan berkelanjutan (ISO, 2018).

Perkembangan konsep enterprise risk management (ERM) semakin memperkuat hubungan antara risiko, strategi, dan kinerja. COSO dalam kerangka 2017 menempatkan manajemen risiko sebagai bagian yang terintegrasi dengan penetapan strategi dan pencapaian kinerja. ERM dipahami sebagai budaya, kapabilitas, dan praktik yang terintegrasi dengan penetapan strategi dan kinerja untuk mengelola risiko dalam menciptakan, mempertahankan, dan merealisasikan nilai (COSO, 2017).

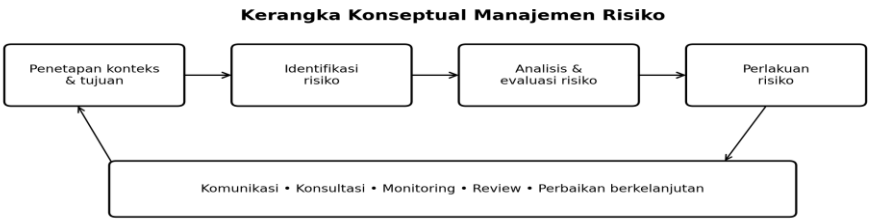
Dalam sektor keuangan, kebutuhan terhadap manajemen risiko menjadi semakin penting karena gangguan operasional, kegagalan teknologi, insiden siber, bencana, dan ketergantungan pada pihak ketiga dapat menimbulkan dampak yang luas. Basel Committee menempatkan governance, operational risk management, business continuity, interdependencies, third-party dependency, incident management, serta ketahanan ICT dan keamanan siber sebagai unsur penting operational resilience (BCBS, 2021).

Atas dasar itu, artikel ini membahas konsep dasar manajemen risiko secara sistematis melalui kajian literatur. Pembahasan diarahkan pada pengertian risiko dan manajemen risiko, prinsip dasar, proses pengelolaan risiko, klasifikasi risiko, integrasi risiko dengan tata kelola dan strategi, serta implikasinya bagi organisasi. Kajian ini diharapkan dapat menjadi dasar konseptual bagi mahasiswa, akademisi, dan praktisi dalam memahami manajemen risiko sebelum mengembangkan model pengukuran atau penelitian empiris.

METODE

Artikel ini menggunakan metode kajian literatur konseptual. Sumber utama meliputi ISO 31000:2018, COSO Enterprise Risk Management–Integrating with Strategy and Performance, prinsip Basel Committee mengenai operational risk dan operational resilience, serta artikel ilmiah yang membahas fondasi risk assessment dan enterprise risk management. Sumber dipilih berdasarkan relevansinya dengan konsep dasar manajemen risiko, kemudian disintesis untuk mengidentifikasi definisi, prinsip, proses, klasifikasi, dan hubungan antara risiko dengan strategi serta kinerja organisasi. Karena artikel bersifat konseptual, tabel dan gambar yang disajikan merupakan hasil sintesis literatur, bukan hasil survei atau pengujian statistik primer.

HASIL DAN PEMBAHASAN



Gambar 1. Siklus dasar manajemen risiko yang terintegrasi

Gambar 1 memperlihatkan bahwa proses manajemen risiko bersifat siklikal. Penetapan konteks menjadi dasar untuk mengidentifikasi risiko; hasil identifikasi kemudian dianalisis dan dievaluasi untuk menentukan respons. Seluruh tahapan tidak berjalan sendiri karena komunikasi, konsultasi, monitoring, review, dan perbaikan berkelanjutan melekat pada keseluruhan proses.

Konsep risiko dan manajemen risiko

Risiko dapat dipahami sebagai dampak ketidakpastian terhadap tujuan. Konsep ini menunjukkan bahwa risiko selalu berkaitan dengan tujuan tertentu; tanpa tujuan, tidak tersedia dasar yang jelas untuk menentukan apakah suatu ketidakpastian relevan. Aven (2016) menunjukkan bahwa kajian risiko berkembang dari pendekatan yang sangat probabilistik menuju perspektif yang juga mempertimbangkan pengetahuan, ketidakpastian, kerentanan, dan konsekuensi. Karena itu, organisasi perlu membedakan antara risiko yang telah diketahui, risiko yang dapat dianalisis dengan data, dan ketidakpastian yang masih memiliki keterbatasan informasi.

Manajemen risiko merupakan rangkaian aktivitas terstruktur untuk mengarahkan dan mengendalikan organisasi berkaitan dengan risiko. ISO 31000:2018 menekankan proses identifikasi, analisis, evaluasi, perlakuan, pemantauan, dan komunikasi risiko. Pendekatan tersebut menunjukkan bahwa manajemen risiko adalah proses berulang, bukan kegiatan satu kali. Hasil evaluasi dapat mengubah perlakuan risiko, sementara perubahan lingkungan dapat memunculkan risiko baru sehingga proses harus diperbarui secara berkelanjutan (ISO, 2018).

Prinsip dasar manajemen risiko

Prinsip pertama adalah integrasi. Risiko harus menjadi bagian dari pengambilan keputusan dan proses organisasi, bukan hanya tanggung jawab unit risk management. Prinsip kedua adalah pendekatan yang terstruktur dan komprehensif agar risiko dapat dibandingkan secara konsisten. Prinsip ketiga adalah penyesuaian dengan konteks, karena profil risiko organisasi berbeda berdasarkan ukuran, industri, struktur, strategi, dan sumber daya. Prinsip berikutnya adalah inklusivitas, yaitu melibatkan pihak yang relevan agar informasi dan perspektif mengenai risiko tidak terlalu sempit. ISO 31000:2018 juga menekankan faktor manusia dan budaya, dinamika perubahan, serta perbaikan berkelanjutan (ISO, 2018).

Tahapan proses manajemen risiko

Proses dimulai dari penetapan konteks dan tujuan. Organisasi perlu memahami lingkungan internal dan eksternal, sasaran, pemangku kepentingan, serta kriteria risiko. Tahap berikutnya adalah identifikasi risiko untuk menemukan sumber, kejadian, penyebab, dan konsekuensi yang dapat menghambat atau memengaruhi tujuan. Setelah itu dilakukan analisis untuk memahami sifat risiko dan tingkatannya, kemudian evaluasi untuk menentukan prioritas berdasarkan kriteria yang telah ditetapkan. Risiko yang memerlukan tindakan selanjutnya diperlakukan melalui pilihan seperti menghindari, mengurangi, membagi atau mentransfer, menerima, dan dalam konteks tertentu mengeksploitasi peluang. Seluruh proses didukung komunikasi, konsultasi, monitoring, dan review (ISO, 2018).

Klasifikasi risiko

Secara konseptual, risiko dapat dikelompokkan sesuai sumber dan karakteristiknya. Risiko strategis berkaitan dengan keputusan bisnis dan perubahan lingkungan yang memengaruhi pencapaian strategi. Risiko operasional berasal dari proses internal, manusia, sistem, teknologi, atau kejadian eksternal. Risiko keuangan mencakup antara lain risiko kredit, pasar, likuiditas, dan risiko yang memengaruhi posisi keuangan. Risiko kepatuhan berkaitan dengan kegagalan memenuhi hukum, regulasi, atau kebijakan. Selain itu terdapat risiko reputasi, teknologi, siber, pihak ketiga, dan risiko keberlanjutan. Kaplan dan Mikes (2012) menunjukkan pentingnya menyesuaikan pendekatan pengelolaan dengan karakter risiko; risiko yang dapat dicegah, risiko strategi, dan risiko eksternal memerlukan mekanisme pengendalian dan pengambilan keputusan yang berbeda.

Integrasi risiko dengan strategi dan tata kelola

Manajemen risiko yang efektif memerlukan dukungan tata kelola. Dewan dan manajemen senior perlu menentukan arah, risk appetite, tanggung jawab, mekanisme eskalasi, dan kualitas pelaporan. COSO menegaskan pentingnya mempertimbangkan risiko dalam proses penetapan strategi dan kinerja, sehingga evaluasi risiko tidak dilakukan setelah strategi selesai (COSO, 2017). Bromiley et al. (2015) juga menekankan bahwa ERM mengarah pada pengelolaan risiko secara terintegrasi dan penyelarasan dengan corporate governance serta strategy.

Di tingkat operasional, integrasi membutuhkan risk register, indikator risiko utama, batas toleransi, pemilik risiko, prosedur eskalasi, dan pelaporan berkala. Dalam sektor perbankan, Basel Committee menekankan budaya risiko, peran board dan senior management, serta kemampuan mengidentifikasi dan menilai kerentanan proses kritis secara berkelanjutan (BCBS, 2021).

Manajemen risiko pada lingkungan digital

Transformasi digital memperluas sumber risiko. Ketergantungan pada sistem informasi, cloud, fintech, analitik data, kecerdasan buatan, dan pihak ketiga dapat meningkatkan efisiensi tetapi sekaligus menciptakan eksposur baru. Risiko dapat muncul dari kegagalan sistem, serangan siber, kualitas data, privasi, model analitik, vendor, dan konsentrasi teknologi. Basel Committee menempatkan resilient ICT, cyber security, third-party dependency, incident management, serta business continuity sebagai elemen penting operational resilience (BCBS, 2021).

Temuan konseptual tersebut menunjukkan bahwa teknologi bukan pengganti manajemen risiko. Teknologi menjadi alat untuk meningkatkan kemampuan deteksi, pengukuran, monitoring, dan respons. Kualitas hasil tetap bergantung pada governance, kompetensi, kualitas data, budaya risiko, dan kejelasan tanggung jawab. Dengan demikian, digital risk management perlu diposisikan sebagai bagian dari enterprise risk management, bukan sebagai fungsi teknologi yang terpisah.

Tabel 1. Sintesis kerangka konsep manajemen risiko

No	Sumber	Fokus konsep	Unsur utama	Konteks
1	ISO 31000:2018	Prinsip & proses generik	Identifikasi–analisis–evaluasi–perlakuan–monitoring	Semua organisasi
2	COSO ERM 2017	Integrasi risiko–strategi–kinerja	Governance, strategy, performance, review, information	Organisasi/korporasi
3	BCBS 2021	Operational risk & resilience	Governance, continuity, ICT, third party, incident	Perbankan
4	Kaplan & Mikes (2012)	Klasifikasi berdasarkan karakter risiko	Preventable, strategy, external	Manajerial
5	Aven (2016)	Fondasi konseptual risiko	Ketidakpastian, pengetahuan, konsekuensi	Lintas disiplin

PEMBAHASAN

Sintesis literatur pada Tabel 1 menunjukkan adanya pergeseran paradigma dari risk management yang bersifat reaktif menuju pendekatan yang terintegrasi dengan strategi. ISO 31000

menyediakan proses generik yang dapat disesuaikan, COSO menekankan hubungan risiko dengan strategy-setting dan performance, sedangkan Basel memberikan penekanan yang lebih spesifik pada ketahanan operasional sektor perbankan. Ketiganya saling melengkapi: ISO memberikan logika proses, COSO memberikan perspektif integrasi organisasi, dan Basel memberikan kedalaman pada risiko operasional serta resilience.

Perbedaan tersebut juga menunjukkan bahwa tidak terdapat satu mekanisme yang dapat digunakan secara identik untuk semua risiko. Risiko yang dapat dicegah membutuhkan pengendalian, standar, dan disiplin proses; risiko strategi membutuhkan dialog dan pengambilan keputusan yang mempertimbangkan trade-off; sedangkan risiko eksternal membutuhkan scenario analysis, early warning, dan kemampuan adaptasi. Perspektif Kaplan dan Mikes (2012) memperkuat argumen bahwa pendekatan risk management harus disesuaikan dengan karakter risiko.

Secara praktis, efektivitas manajemen risiko dapat dinilai dari kemampuan organisasi menghubungkan empat unsur: tujuan, risiko, respons, dan hasil. Organisasi yang hanya memiliki daftar risiko tanpa pemilik, indikator, batas toleransi, dan mekanisme tindak lanjut belum tentu memiliki sistem manajemen risiko yang efektif. Sebaliknya, sistem yang menghubungkan risk appetite dengan strategi, anggaran, indikator kinerja, dan monitoring memungkinkan manajemen mengambil keputusan yang lebih konsisten. Hal ini sejalan dengan gagasan ERM bahwa risiko perlu diintegrasikan dengan penciptaan dan perlindungan nilai (COSO, 2017).

Untuk organisasi yang mengalami digitalisasi, dimensi risiko juga menjadi lebih dinamis. Kecepatan perubahan teknologi dapat membuat profil risiko berubah sebelum prosedur lama diperbarui. Karena itu, monitoring berkelanjutan, incident reporting, business continuity testing, dan pengelolaan ketergantungan pihak ketiga menjadi semakin penting. Basel Committee secara eksplisit memasukkan interconnections, third-party dependency, incident management, serta resilient ICT dalam operational resilience (BCBS, 2021).

Implikasi akademiknya adalah konsep manajemen risiko dapat dijadikan landasan untuk mengembangkan konstruk yang lebih spesifik, misalnya risk governance, digital risk management, ESG risk management, climate risk management, atau risk-adjusted performance. Namun, pengembangan konstruk tersebut tetap perlu menjaga prinsip dasar bahwa risiko harus dikaitkan dengan tujuan, konteks, sumber ketidakpastian, kriteria evaluasi, dan respons organisasi.

SIMPULAN

Konsep dasar manajemen risiko menunjukkan bahwa risiko merupakan bagian inheren dari pengambilan keputusan dalam kondisi ketidakpastian. Manajemen risiko yang efektif tidak berhenti pada identifikasi ancaman, tetapi mengintegrasikan penetapan tujuan, analisis dan evaluasi risiko, perlakuan, monitoring, komunikasi, serta perbaikan berkelanjutan ke dalam tata kelola dan strategi organisasi. Sintesis ISO 31000, COSO ERM, Basel Committee, dan literatur akademik memperlihatkan bahwa pendekatan risiko perlu disesuaikan dengan karakter risiko dan konteks organisasi. Dalam lingkungan digital, cakupan manajemen risiko semakin luas karena munculnya risiko siber, teknologi, data, pihak ketiga, dan ketergantungan sistem. Oleh karena itu, fondasi manajemen risiko yang kuat membutuhkan kepemimpinan, budaya risiko, informasi yang berkualitas, kejelasan tanggung jawab, serta mekanisme monitoring yang adaptif.

REFERENSI

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. Long Range Planning, 48(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management—Integrating with strategy and performance. COSO.

International Organization for Standardization. (2018). ISO 31000:2018 Risk management—Guidelines. ISO.

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. Harvard Business Review, 90(6), 48–60.