FISKAL : Jurnal Ekonomi, Bisnis dan Manajemen
ISSN: 3090-0328
Volume 2 Nomor 2 Tahun 2026
https://ejournal.almusthofa.org/index.php/fiskal/index

IDENTIFIKASI DAN MITIGASI RESIKO OPERASIONAL PADA PERUSAHAAN E-COMMERCE

Natasya Andini[1], Winsi Ulaini[2]
[12]Universitas Islam Negeri Fatmawati Sukarno Bengkulu
natasyaandini220805@gmail, winsiulaini@gmail.com

ABSTRAK

Perkembangan sektor e-commerce memaksa perusahaan untuk meningkatkan efektivitas operasional serta kemampuan mereka dalam menghadapi risiko. Risiko operasional yang dihadapi oleh perusahaan e-commerce termasuk gangguan sistem, kesalahan manusia, keterlambatan dalam pengiriman, kebocoran informasi pelanggan, dan penipuan dalam transaksi online. Tujuan dari penelitian ini adalah untuk mengidentifikasi berbagai risiko operasional dan menganalisis langkah-langkah mitigasi yang diadopsi oleh perusahaan e-commerce. Pendekatan yang digunakan dalam penelitian ini adalah kualitatif deskriptif dengan metode studi pustaka. Data yang dikumpulkan berasal dari berbagai sumber sekunder seperti artikel ilmiah, buku, laporan penelitian, dan dokumen lain yang berkaitan dengan manajemen risiko operasional dalam perusahaan e-commerce. Temuan penelitian mengungkapkan bahwa risiko utama meliputi gangguan pada server, keterlambatan dalam distribusi, kesalahan dalam pengelolaan inventaris, dan kebocoran informasi pelanggan. Beberapa strategi mitigasi yang diterapkan antara lain adalah penguatan keamanan siber, peningkatan pengawasan dalam rantai pasok, pelatihan untuk karyawan, pemanfaatan cadangan data, dan penerapan prosedur operasional standar yang tepat. Penelitian ini diharapkan dapat memberikan referensi bagi perusahaan e-commerce dalam meningkatkan pengelolaan risiko operasional dan menjaga kepercayaan dari pelanggan.

Kata Kunci: *risiko operasional, e-commerce, mitigasi risiko, manajemen risiko.*

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong laju pertumbuhan bisnis digital, terutama dalam sektor perdagangan elektronik atau e-commerce. E-commerce menjadi salah satu inovasi dalam dunia bisnis yang memudahkan transaksi, memperluas akses pasar, dan meningkatkan efisiensi operasional perusahaan. Melalui platform digital, perusahaan dapat menawarkan produk dan layanan dengan cara yang lebih cepat dan fleksibel kepada pelanggan.

Namun, meskipun menawarkan banyak kemudahan, perusahaan e-commerce juga harus menghadapi berbagai risiko operasional yang dapat mengancam kelangsungan usaha. Di antara risiko ini terdapat gangguan pada sistem informasi, kebocoran data pelanggan, salah pengelolaan persediaan, keterlambatan dalam pengiriman, dan potensi serangan siber. Jika risiko operasional ini tidak dikelola dengan baik, hal tersebut dapat menurunkan kualitas layanan, mengakibatkan kerugian finansial bagi perusahaan, serta mengurangi kepercayaan pelanggan terhadap platform e-commerce.

Penelitian tentang risiko operasional di perusahaan e-commerce telah banyak dilakukan. Namun, sebagian besar penelitian sebelumnya umumnya lebih terfokus pada isu keamanan teknologi dan transaksi digital. Sementara itu, kajian yang membahas risiko operasional secara menyeluruh—yang mencakup aspek teknologi informasi, sumber daya manusia, proses bisnis, serta strategi untuk mitigasi—masih sangat terbatas. Oleh karena itu,

diperlukan studi yang dapat memberikan pemahaman lebih dalam mengenai identifikasi dan pengurangan risiko operasional di perusahaan e-commerce.

Tujuan dari penelitian ini adalah untuk mengidentifikasi beragam risiko operasional yang dihadapi perusahaan e-commerce serta menganalisis strategi mitigasi yang dapat digunakan untuk meminimalkan efek risiko tersebut. Diharapkan, hasil dari penelitian ini bisa menjadi referensi bagi perusahaan e-commerce dalam meningkatkan efektivitas manajemen risiko operasional dan menjaga kepercayaan pelanggan di era digital saat ini.

METODE PENELITIAN

Penelitian ini menerapkan pendekatan kualitatif deskriptif dengan menggunakan metode studi pustaka. Metode ini bertujuan untuk memahami serta menganalisis berbagai konsep, teori, dan temuan penelitian sebelumnya yang berkaitan dengan risiko operasional dan strategi pengurangi risiko dalam perusahaan e-commerce.

Informasi yang digunakaan dalam penelitian ini adalah data sekunder yang diperoleh dari jurnal ilmiah baik nasional maupun internasional, buku, laporan penelitian, prosiding seminar, dan dokumen lain yang terkait dengan topik yang diteliti. Sumber yang dipilih didasarkan pada relevansi, kredibilitas, dan keaktualan informasi, agar hasil penelitian sejalan dengan perkembangan bisnis digital saat ini.

Pengumpulan data dilakukan melalui langkah-langkah identifikasi, seleksi, pencatatan, dan pengelompokan literatur yang relevan dengan risiko operasional, manajemen risiko, e-commerce, dan pengurangan risiko. Selanjutnya, data tersebut dianalisis dengan menggunakan teknik analisis isi secara tematik untuk menemukan pola, hubungan, dan strategi pengurangan risiko operasional yang diimplementasikan dalam perusahaan e-commerce.

HASIL DAN PEMBAHASAN

Pengidentifikasian Risiko Operasional di Perusahaan E-Commerce

Temuan dari penelitian menunjukkan bahwa risiko operasional di perusahaan e-commerce disebabkan oleh tiga faktor utama, yaitu teknologi informasi, sumber daya manusia, dan proses bisnis. Risiko yang berkaitan dengan teknologi informasi dapat diidentifikasi melalui masalah server, kegagalan sistem transaksi, dan ancaman serangan siber yang bisa mengganggu kelangsungan layanan. Hal ini menunjukkan bahwa e-commerce sangat bergantung pada sistem digital dalam semua aktivitas operasionalnya.

Di sisi lain, risiko dalam aspek sumber daya manusia muncul dalam bentuk kesalahan input data, ketidakakuratan dalam pengelolaan informasi, dan kesalahan yang dilakukan oleh manusia selama proses administrasi. Sedangkan pada aspek proses bisnis, risiko terlihat dari ketidaksesuaian informasi produk, kesalahan dalam pengelolaan stok, serta keterlambatan dalam pemrosesan pesanan. Secara keseluruhan, hasil penelitian ini menunjukkan bahwa kompleksitas sistem e-commerce menjadikan perusahaan lebih mudah terkena risiko operasional (Hopkin, 2018).

Dalam hal teknologi informasi, risiko operasional umumnya muncul dalam bentuk masalah dengan server, kegagalan sistem saat memproses transaksi, kesalahan pada aplikasi, dan ancaman terhadap keamanan siber seperti peretasan, virus, penipuan online, serta pencurian data pelanggan. Risiko ini dapat muncul akibat keamanan jaringan yang lemah, kurangnya pembaruan perangkat lunak, atau volume transaksi digital yang tinggi secara berkelanjutan. Ketika terjadi gangguan sistem, perusahaan dapat mengalami kejatuhan dalam kinerja operasional yang berpengaruh langsung pada proses transaksi bagi pelanggan. Di

samping itu, kebocoran data pelanggan merupakan ancaman serius karena bisa berujung pada kerugian finansial dan menurunkan kepercayaan konsumen terhadap platform e-commerce.

Selain itu, temuan dari penelitian juga mengungkapkan bahwa perusahaan e-commerce menghadapi ancaman dari pihak eksternal seperti mitra pengiriman, penyedia teknologi, serta perubahan perilaku konsumen di pasar digital. Ketergantungan pada pihak ketiga dalam proses pengiriman produk mempersulit perusahaan untuk menjaga mutu layanan secara keseluruhan (Chopra dan Meindl, 2019). Jika terjadi keterlambatan pengiriman atau kerusakan barang selama proses distribusi, perusahaan e-commerce akan tetap merasakan dampak negatif berupa keluhan dari pelanggan dan penurunan kepercayaan dari konsumen.

Klasifikasi Risiko Operasional

Dari analisis yang dilakukan, risiko operasional dapat dibagi menjadi tiga kategori, yaitu risiko yang berkaitan dengan teknologi informasi, risiko yang terjadi di dalam perusahaan, dan risiko yang berasal dari faktor eksternal. Risiko yang berkaitan dengan teknologi informasi termasuk permasalahan pada server, kesalahan dalam sistem, dan ancaman terhadap keamanan data pelanggan yang terkait dengan risiko siber.

Risiko yang terjadi di dalam perusahaan berkaitan dengan aktivitas internal, seperti kesalahan dalam pengelolaan stok, ketidakakuratan saat memasukkan informasi, serta lemahnya pengawasan dalam organisasi. Sedangkan, risiko yang berasal dari luar mencakup masalah eksternal, termasuk keterlambatan pengiriman, gangguan dari pihak ketiga, dan perubahan dalam perilaku konsumen (Haryanti, 2024).

Pengelompokan ini sangat krusial agar perusahaan dapat lebih memahami sumber olahraga risiko dengan jelas, sehingga langkah-langkah untuk mengurangi risiko bisa dilakukan dengan lebih terarah dan efisien.

Risiko operasional yang terdapat di perusahaan berkaitan dengan aktivitas yang berlangsung di dalam organisasi, seperti kesalahan dalam manajemen persediaan, ketidakakuratan dalam penginputan data, kesalahan administratif, pengawasan internal yang lemah, serta kurang efektifnya koordinasi antar berbagai divisi perusahaan (Hanafi, 2018). Kesalahan dalam pengelolaan persediaan dapat menyebabkan adanya perbedaan antara jumlah barang yang ada secara fisik dengan catatan yang ada dalam sistem perusahaan.

Hal ini bisa mengganggu proses distribusi barang dan menyebabkan penundaan dalam pengiriman kepada pelanggan. Selain itu, lemahnya pengawasan internal juga dapat meningkatkan risiko penipuan yang bisa merugikan perusahaan baik dari sisi finansial maupun operasional (Darmawi, 2016).

Analisis Dampak Risiko terhadap Operasional Perusahaan

Risiko yang berkaitan dengan operasional memiliki dampak signifikan terhadap performa perusahaan e-commerce. Gangguan pada sistem informasi dapat mengakibatkan penghentian transaksi untuk waktu tertentu, yang berimbas pada penurunan pemasukan perusahaan. Ini menunjukkan bahwa keberlangsungan sistem digital sangat penting bagi stabilitas operasional dari bisnis (Pavlou, 2003). Selain itu, kebocoran data pelanggan dapat merusak tingkat kepercayaan konsumen terhadap platform e-commerce.

Di dalam dunia bisnis digital, kepercayaan menjadi elemen utama dalam membangun loyalitas di antara konsumen. Keterlambatan dalam pengiriman juga berdampak negatif pada tingkat kepuasan pelanggan, yang pada akhirnya dapat memengaruhi reputasi perusahaan di pasar digital.

Selain menghambat transaksi, masalah dalam sistem teknologi informasi juga dapat meningkatkan biaya operasional bagi perusahaan. Ketika server mengalami kerusakan atau ada gangguan jaringan, perusahaan harus mengeluarkan biaya tambahan untuk memperbaiki sistem, memulihkan data, dan memperkuat keamanan teknologi informasi (Turban et al. , 2018). Dalam situasi tertentu, perusahaan bahkan harus menghentikan sementara operasi untuk melakukan perawatan sistem, yang tentu saja berdampak pada penurunan produktivitas perusahaan.

Strategi Penanganan Risiko Operasional

Temuan dari penelitian menunjukkan bahwa perusahaan e-commerce telah menerapkan berbagai strategi untuk mengatasi risiko. Strategi pertama adalah memperkuat keamanan sistem informasi dengan menerapkan enkripsi data, firewall, dan sistem verifikasi identitas untuk mencegah akses yang tidak sah. Tindakan ini sesuai dengan prinsip pengendalian risiko teknologi informasi yang tercantum dalam standar manajemen risiko (Haryanti, 2024).

Strategi kedua melibatkan pelaksanaan sistem pencadangan secara berkala untuk mengurangi dampak kehilangan data akibat gangguan sistem. Strategi ketiga berfokus pada peningkatan kemampuan tenaga kerja melalui program pelatihan untuk meminimalkan kesalahan manusia dalam operasional. Selain itu, perusahaan juga memperhatikan pengawasan terhadap rantai pasokan dan mitra logistik guna mengurangi kemungkinan keterlambatan dalam proses distribusi. Penerapan SOP (Prosedur Operasional Standar) digunakan sebagai pedoman kerja untuk meningkatkan konsistensi dalam proses operasional (Heizer, Render, dan Munson, 2017).

Dalam praktiknya, perusahaan e-commerce dapat memanfaatkan sistem verifikasi dua faktor dan enkripsi data untuk meningkatkan keamanan akun pengguna dan melindungi data pelanggan dari ancaman kebocoran informasi. Di samping itu, perusahaan juga bisa menerapkan sistem pemantauan server secara langsung agar gangguan teknis dapat segera diidentifikasi dan diatasi sebelum mengganggu transaksi pelanggan.

Dalam hal pengelolaan persediaan dan distribusi, penggunaan sistem inventaris otomatis dapat membantu perusahaan mengurangi kesalahan dalam pencatatan barang dan meningkatkan ketepatan data persediaan. Perusahaan juga bisa memanfaatkan sistem pelacakan pengiriman untuk memantau proses distribusi dengan lebih efisien, sehingga keterlambatan pengiriman dapat diminimalkan.

Penilaian Efektivitas Penanganan Risiko

Penilaian menunjukkan bahwa penggunaan strategi untuk menghadapi risiko memberikan pengaruh positif dalam mengurangi gangguan dalam operasional. Peningkatan sistem keamanan informasi dapat menurunkan potensi bocornya data pelanggan, sementara pemanfaatan data cadangan memperkuat sistem terhadap gangguan teknis.

Namun, masih ada beberapa kelemahan seperti ketergantungan pada pihak ketiga dalam pengaturan logistik dan kesalahan yang dibuat oleh manusia dalam pengelolaan data. Ini mengindikasikan bahwa pengelolaan risiko operasional harus bersifat progresif dan harus terus diperbarui sejalan dengan perkembangan teknologi serta kompleksitas bisnis (Hopkin, 2018).

Oleh karena itu, penerapan manajemen risiko yang terstruktur dapat meningkatkan efisiensi operasional dan tetap menjaga kepercayaan pelanggan terhadap perusahaan e-commerce. Ini menunjukkan bahwa manajemen risiko operasional harus fleksibel dan berkelanjutan, bukan dalam bentuk yang statis. Perusahaan diwajibkan untuk secara berkala

melakukan evaluasi, memperbarui sistem yang ada, dan menyesuaikan strategi untuk menghadapi risiko sesuai dengan perkembangan teknologi dan kompleksitas yang meningkat dalam dunia bisnis e-commerce. Pendekatan yang adaptif terhadap perubahan dalam lingkungan bisnis menjadi unsur penting untuk menjaga efektivitas pengelolaan risiko operasional.

Risiko operasional yang tidak dikelola dengan baik dapat memberikan dampak jangka panjang yang serius bagi perusahaan, terutama pada sektor digital seperti e-commerce dan layanan berbasis teknologi. Risiko operasional tidak hanya berkaitan dengan gangguan sistem, kesalahan manusia, atau kegagalan prosedur internal, tetapi juga mencakup ancaman keamanan siber, kebocoran data, serta lemahnya pengawasan terhadap infrastruktur teknologi informasi. Dalam era ekonomi digital, data pelanggan merupakan aset strategis perusahaan sehingga gangguan terhadap keamanan data dapat menimbulkan konsekuensi multidimensional, baik secara finansial maupun nonfinansial.

Sebagai contoh, kebocoran data pelanggan tidak hanya menimbulkan kerugian finansial akibat biaya pemulihan sistem, kompensasi kepada konsumen, maupun potensi sanksi regulator, tetapi juga dapat merusak reputasi perusahaan secara signifikan. Dalam konteks bisnis digital, reputasi dan kepercayaan merupakan modal utama dalam mempertahankan loyalitas konsumen. Ketika pelanggan merasa data pribadinya tidak aman, maka tingkat kepercayaan terhadap platform akan menurun dan mendorong konsumen untuk beralih kepada kompetitor yang dianggap lebih mampu menjamin keamanan transaksi. Kondisi ini menunjukkan bahwa risiko operasional memiliki keterkaitan langsung dengan risiko reputasi dan risiko bisnis secara keseluruhan.

Fenomena tersebut semakin relevan karena karakteristik transaksi digital sangat bergantung pada trust atau kepercayaan konsumen. Penelitian mengenai e-commerce menunjukkan bahwa keamanan data, privasi, dan reliabilitas platform merupakan faktor utama yang memengaruhi keputusan konsumen dalam melakukan transaksi online. (arXiv) Ketika terjadi pelanggaran keamanan atau data breach, konsumen tidak hanya mengalami kekhawatiran terhadap penyalahgunaan data pribadi, tetapi juga mulai meragukan kredibilitas perusahaan dalam mengelola sistem digitalnya. Akibatnya, perusahaan dapat mengalami penurunan jumlah pengguna aktif, melemahnya loyalitas pelanggan, hingga turunnya volume transaksi dalam jangka panjang.

Kasus kebocoran data pada beberapa platform e-commerce besar menunjukkan bahwa dampak risiko operasional dapat meluas hingga memengaruhi keberlanjutan bisnis perusahaan. Kebocoran jutaan data pelanggan pada platform digital di Indonesia memperlihatkan bagaimana kelemahan sistem keamanan dapat menjadi ancaman serius bagi industri digital. (Artikel Rechtsvinding) Selain menyebabkan kerugian ekonomi, insiden tersebut juga memunculkan persepsi negatif masyarakat terhadap keamanan transaksi digital. Dalam jangka panjang, kondisi ini dapat menghambat pertumbuhan ekosistem ekonomi digital karena masyarakat menjadi lebih berhati-hati dalam menggunakan layanan berbasis online.

Dari perspektif manajemen risiko, kondisi tersebut menunjukkan pentingnya penerapan operational risk management yang terintegrasi dan berbasis teknologi. Perusahaan tidak cukup hanya mengandalkan sistem keamanan dasar, tetapi harus membangun mekanisme mitigasi risiko yang komprehensif melalui penguatan cyber security, audit sistem berkala, enkripsi data, disaster recovery system, serta peningkatan kompetensi sumber daya manusia di bidang keamanan digital. Regulasi dan pengawasan dari lembaga seperti Otoritas Jasa Keuangan juga menjadi faktor penting dalam memastikan perusahaan memiliki standar perlindungan data dan keamanan sistem yang memadai. (OJK Portal)

Selain itu, perusahaan perlu memahami bahwa dampak risiko operasional bersifat akumulatif dan dapat berkembang menjadi krisis kepercayaan publik apabila tidak ditangani secara cepat dan transparan. Dalam banyak kasus, kegagalan perusahaan dalam memberikan respons yang jelas terhadap insiden kebocoran data justru memperbesar ketidakpercayaan masyarakat. Oleh karena itu, strategi komunikasi krisis, transparansi informasi, serta kecepatan penanganan insiden menjadi bagian penting dalam manajemen risiko operasional modern.

Dengan demikian, pengelolaan risiko operasional dalam perusahaan digital tidak lagi hanya dipandang sebagai fungsi teknis semata, melainkan telah menjadi bagian strategis dalam menjaga keberlangsungan usaha, reputasi perusahaan, dan kepercayaan konsumen. Perusahaan yang mampu membangun sistem keamanan dan tata kelola risiko yang baik akan memiliki daya saing lebih kuat dalam menghadapi dinamika industri digital yang semakin kompetitif dan rentan terhadap ancaman siber.

Di samping itu, penerapan prosedur operasional standar (SOP) serta pelatihan bagi sumber daya manusia terbukti membantu mengurangi kesalahan yang ditimbulkan oleh manusia dalam proses operasional. Namun demikian, efektivitas strategi tersebut tetap bergantung pada konsistensi pengawasan dan kemampuan perusahaan untuk menyesuaikan sistem manajemen risiko dengan perkembangan teknologi serta kebutuhan dalam bisnis digital. Dengan demikian, penerapan manajemen risiko yang terencana dan berkelanjutan tidak hanya dapat mengurangi kemungkinan gangguan dalam operasional, tetapi juga dapat meningkatkan efisiensi kerja perusahaan, menjaga kepercayaan konsumen, dan memperkuat daya saing perusahaan e-commerce di pasar digital yang semakin kompetitif (Laudon dan Traver, 2021).

KESIMPULAN

Berdasarkan hasil studi dan analisis, dapat disimpulkan bahwa risiko operasional yang dihadapi oleh perusahaan e-commerce dipengaruhi oleh berbagai faktor, seperti teknologi informasi, sumber daya manusia, proses bisnis, serta faktor eksternal termasuk pihak ketiga dan perubahan dalam perilaku konsumen. Risiko ini mencakup masalah pada server, kegagalan sistem transaksi, ancaman siber, kesalahan dalam memasukkan data, ketidaksesuaian informasi produk, kesalahan dalam pengelolaan stok, dan keterlambatan pengiriman yang dapat mengurangi kualitas layanan, menurunkan kepercayaan pelanggan, serta mempengaruhi kinerja perusahaan. Penelitian ini juga menunjukkan bahwa perusahaan e-commerce sangat bergantung pada sistem digital dan mitra logistik, sehingga membuatnya lebih rentan terhadap terjadinya gangguan operasional. Untuk mengurangi risiko ini, perusahaan menggunakan berbagai strategi seperti memperkuat keamanan sistem informasi dengan enkripsi data, firewall, otentikasi dua langkah, pencadangan data, penerapan standar operasional prosedur, pelatihan bagi sumber daya manusia, pemanfaatan sistem inventaris otomatis, serta pemantauan rantai pasokan dan distribusi. Strategi tersebut terbukti efektif dalam mengurangi gangguan operasional dan meningkatkan pengelolaan risiko, meskipun masih ada kelemahan seperti ketergantungan pada pihak ketiga dan kemungkinan terjadinya kesalahan manusia. Oleh karena itu, perusahaan perlu menerapkan manajemen risiko operasional yang fleksibel, terencana, dan berkelanjutan untuk meningkatkan efisiensi operasional, menjaga kepercayaan konsumen, dan memperkuat posisi kompetitif perusahaan.

REFERENSI

Prasetio, A., Ashoer, M., Hutahaean, J., Simarmata, J., Samosir, R. S., Nugraha, H., & Manullang, S. O. (2021). Konsep dasar e-commerce. Yayasan Kita Menulis.

Rahayu, P., & Rangkuti, S. (2022). Analisis manajemen risiko penggunaan aplikasi e-commerce dalam transaksi penjualan CV. Roti Aroma Bakery dan Cake Shop Medan. Bisnis-Net Jurnal Ekonomi dan Bisnis, 5(1), 55–68.

Pujawan, I. N., & Geraldin, L. H. (2009). House of risk: A model for proactive supply chain risk management.

Heizer, J., Render, B., & Munson, C. (2017). Operations management: Sustainability and supply chain management.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model.

Haryanti, D. R. (2024). Analisis manajemen risiko operasional berbasis ISO 31000:2018 terhadap perusahaan logistik. Jurnal Simki Economic, 7(2), 631–642.

Hopkin, P. (2018). Fundamentals of risk management: Understanding, evaluating and implementing effective risk management. Kogan Page Publishers.

Chopra, S., & Meindl, P. (2019). Supply chain management: Strategy, planning, and operation. Pearson Education.

Hanafi, M. M. (2018). Manajemen risiko. UPP STIM YKPN.

Darmawi, H. (2016). Manajemen risiko. Bumi Aksara.

Turban, E., Pollard, C., & Wood, G. (2018). Information technology for management: On-demand strategies for performance, growth and sustainability. Wiley.