MUSYTARI
ISSN : 3025-9495

Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

PENERAPAN SISTEM INFORMASI MANAJEMEN DALAM MENINGKATKAN MANAJEMENRISIKO DAN KEAMANAN INFORMASI

Isnaini Nur Harahap, Muhammad Irwan Padli Nasution
Fakultas Ekonomi Dan Bisnis Islam, Prodi Manajemen,
Universitas Islam Negeri Sumatera Utara
Email: isnaininurharahap@gmail.com, irwannst@uinsu.ac.id

Abstract

In today's digital era, risk management and information security are critical elements for an organization's operational sustainability. The implementation of Management Information Systems (MIS) plays an important role in supporting these efforts by providing integrated tools and methods to identify, analyze and mitigate various risks related to data and information security. This study aims to determine the effectiveness of the implementation of Management Information Systems in improving risk management and information security in organizations, as well as identifying factors that influence its success. This research method adopts a qualitative approach using case studies to analyze the implementation of Management Information Systems (MIS).
The results show that a well-structured and managed SIM is able to improve early detection of potential threats, accelerate the risk mitigation process, and support compliance with applicable security regulations.

Keywords: Management Information System, Risk Management, Information Security, Information Technology, Compliance

Abstrak

Dalam era digital saat ini, pengelolaan risiko dan keamanan informasi menjadi elemen penting bagi keberlangsungan operasional organisasi. Penerapan Sistem Informasi Manajemen (SIM) memainkan peran penting dalam mendukung upaya ini dengan menyediakan alat dan metode yang terintegrasi untuk mengidentifikasi, menganalisis, dan memitigasi berbagai risiko yang berkaitan dengan data dan keamanan informasi. Penelitian ini bertujuan untuk mengetahui efektivitas penerapan Sistem Informasi Manajemen dalam meningkatkan risiko manajemen dan keamanan informasi dalam organisasi, serta mengidentifikasi faktor-faktor yang mempengaruhi keberhasilannya. Metode penelitian ini mengadopsi pendekatan kualitatif dengan menggunakan studi kasus untuk menganalisis penerapan Sistem Informasi Manajemen (SIM) Hasil penelitian menunjukkan bahwa SIM yang terstruktur dan dikelola dengan baik mampu meningkatkan deteksi dini terhadap potensi ancaman, mempercepat proses mitigasi risiko, serta mendukung kepatuhan terhadap regulasi keamanan yang berlaku. Penelitian ini menyimpulkan bahwa SIM yang diterapkan

Article History
Received: Desember 2024
Reviewed: Desember 2024
Published: Desember 2024

Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/CAUSA.v1i2.365
Copyright : Author
Publish by : Musytari

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

secara efektif dapat menjadi alat strategi dalam meningkatkan keamanan informasi dan mengelola risiko secara proaktif. Temuan ini diharapkan dapat memberikan panduan bagi organisasi dalam merancang strategi manajemen risiko dan keamanan informasi yang lebih baik melalui penerapan SIM yang optimal.
Kata kunci: Sistem Informasi Manajemen, Manajemen Risiko, Keamanan Informasi, Teknologi Informasi, Kepatuhan

1. Pendahuluan

Di era digital yang semakin kompleks, informasi menjadi salah satu aset terpenting bagi organisasi, baik di sektor publik maupun swasta. Dengan kemajuan teknologi, jumlah data yang dikelola oleh perusahaan meningkat pesat, begitu pula dengan risiko keamanan yang menyertainya. Keamanan informasi menjadi perhatian utama bagi organisasi karena ancaman, seperti pencurian data, peretasan, dan kerusakan sistem, dapat berdampak besar pada keberlangsungan operasional dan reputasi perusahaan (Dhillon & Backhouse, 2001). Pentingnya penerapan Sistem Informasi Manajemen (SIM) yang andal untuk mendukung pengelolaan risiko dan menjaga keamanan informasi secara efektif.

Sistem Informasi Manajemen (SIM) merupakan sistem yang dirancang untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi yang diperlukan dalam pengambilan keputusan manajerial. SIM tidak hanya berfungsi sebagai alat untuk meningkatkan efisiensi operasional, tetapi juga sebagai sarana untuk mendeteksi dan mengelola risiko secara lebih proaktif (Laudon & Laudon, 2014). Penerapan SIM yang terstruktur memungkinkan organisasi untuk mendeteksi potensi ancaman dan risiko lebih dini, mengidentifikasi akar masalah, serta mengambil tindakan pencegahan yang sesuai sebelum masuk ke dalam

Manajemen risiko dan keamanan informasi adalah dua aspek yang saling terkait dan memerlukan perhatian khusus dalam strategi perusahaan. Manajemen risiko membantu organisasi mengidentifikasi dan meminimalkan kemungkinan terjadinya ancaman yang dapat mengganggu operasional bisnis. Di sisi lain, keamanan informasi bertujuan untuk melindungi data dan aset digital organisasi dari akses yang tidak sah dan ancaman eksternal. Aspek kedua ini menjadi lebih efektif jika didukung oleh teknologi yang terintegrasi dan sistematis melalui penerapan SIM

Namun penerapan SIM dalam pengelolaan risiko dan keamanan informasi masih menahan berbagai tantangan. Faktor-faktor seperti kurangnya pemahaman tentang teknologi, resistensi terhadap perubahan, dan keterbatasan anggaran sering kali menjadi penghambat dalam penerapan SIM yang optimal (Rogers, 2003). Oleh karena itu, penelitian ini bertujuan untuk menganalisis bagaimana penerapan SIM dapat mendukung pengelolaan risiko dan keamanan informasi, serta mengidentifikasi faktor-faktor yang mempengaruhi efektivitas penerapan tersebut.

Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan strategi manajemen risiko dan keamanan informasi di lingkungan organisasi dengan memanfaatkan SIM secara optimal. Temuan dari penelitian ini dapat digunakan sebagai pedoman bagi perusahaan dalam meningkatkan kemampuan mereka untuk melindungi aset informasi serta mengelola risiko yang dapat mengancam keberlanjuan

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

2. Metode Penelitian

Metode penelitian ini mengadopsi pendekatan kualitatif dengan menggunakan studi kasus untuk menganalisis penerapan Sistem Informasi Manajemen (SIM) dalam meningkatkan manajemen risiko dan keamanan informasi di berbagai organisasi. Pendekatan ini dipilih untuk mendapatkan pemahaman yang lebih mendalam mengenai proses, tantangan, dan manfaat dari penerapan SIM dalam situasi nyata.

3. Hasil dan Pembahasan

a. Definisi Sistem Informasi Manajemen (SIM)

Sistem Informasi Manajemen (SIM) adalah sistem yang dirancang untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi yang diperlukan oleh manajemen suatu organisasi dalam proses pengambilan keputusan (Laudon & Laudon, 2014). SIM mencakup perangkat keras dan perangkat lunak yang memungkinkan manajer dan karyawan untuk berkomunikasi, mengakses informasi, dan melakukan analisis yang diperlukan dalam pengelolaan risiko dan keamanan informasi (O'Brien & Marakas, 2010).

b. Manajemen Risiko dalam Keamanan Informasi

Manajemen risiko adalah serangkaian proses yang digunakan untuk mengidentifikasi, menganalisis, dan mengurangi risiko yang dihadapi oleh organisasi, terutama yang berkaitan dengan data dan informasi (ISO 31000). Proses ini meliputi langkah-langkah seperti identifikasi risiko, analisis dampak, pemilihan metode mitigasi, serta pemantauan dan evaluasi. Penerapan
SIM dapat memperkuat manajemen risiko dengan menyediakan data yang akurat, alat analisis risiko yang mendalam, dan integrasi antar departemen untuk mempercepat respons terhadap ancaman (Boehm, 2011).

c. Keamanan Informasi dan Standar Keamanan

Informasi mencakup berbagai kebijakan, prosedur, dan pengendalian yang dirancang untuk melindungi informasi dari ancaman baik internal maupun eksternal. Informasi keamanan standar, seperti ISO 27001 dan NIST SP 800-53, menyediakan kerangka kerja yang dapat digunakan untuk melindungi data dari akses yang tidak sah, kerusakan, atau kehilangan (Dhillon & Backhouse, 2001). Penerapan SIM memungkinkan organisasi untuk menghubungkan akses dan aktivitas di jaringan mereka secara real-time, mengidentifikasi anomali yang menunjukkan potensi ancaman, serta melindungi data sensitif melalui teknik enkripsi dan kontrol akses otomatis (Whitman & Mattord, 2012).

d. Penerapan Teknologi dalam SIM untuk Keamanan Informasi

Teknologi seperti enkripsi data, otentikasi multifaktor, dan firewall merupakan elemen penting dalam SIM untuk menjaga keamanan informasi. Menurut Chen dkk. (2012), penerapan teknologi ini membantu organisasi dalam meningkatkan keamanan dengan membatasi akses hanya kepada pihak yang berwenang dan memastikan kerahasiaan, integritas, serta ketersediaan informasi. Dengan SIM yang efektif, organisasi dapat menerapkan berbagai fitur keamanan secara efisien, memudahkan pemantauan dan evaluasi informasi keamanan.

e. Integrasi Sistem dan Efisiensi Manajemen Risiko

SIM yang terintegrasi memungkinkan organisasi untuk mengelola risiko secara menyeluruh, dengan menggabungkan data dari berbagai sumber untuk memberikan gambaran yang lengkap tentang risiko yang dihadapi. Sistem Informasi Manajemen yang efektif membantu dalam mendeteksi risiko lebih awal dan memberikan wawasan kepada manajemen mengenai tindakan mitigasi yang diperlukan (McFarlan & Nolan, 2003). Dengan alat pemantauan otomatis, risiko dapat diidentifikasi lebih awal, sementara solusi

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

dapat diterapkan untuk mengurangi dampaknya terhadap operasi bisnis.

f. Dampak Penerapan SIM terhadap Manajemen Risiko dan Keamanan Informasi

Penerapan SIM yang efektif memiliki dampak signifikan terhadap informasi keamanan dan manajemen risiko. Dengan akses informasi secara real-time dan kemampuan untuk menyatukan data di seluruh organisasi, SIM mendukung deteksi dini, pencegahan pelanggaran keamanan, dan pengelolaan kejadian yang efisien. Sistem yang baik juga mengurangi risiko kesalahan manusia dalam pengelolaan data dan meningkatkan transparansi, sehingga memudahkan dalam memenuhi regulasi keamanan (Turban, Leidner, McLean, & Wetherbe, 2008).

g. Kerangka Teori dan Konsep yang Mendukung SIM

Kerangka teori seperti Teori Difusi Inovasi (Rogers, 2003) dan Model Penerimaan Teknologi (Davis, 1989) dapat digunakan untuk memahami faktor-faktor yang mempengaruhi penerimaan dan penggunaan SIM dalam organisasi. Faktor-faktor seperti persepsi kemudahan penggunaan, persepsi manfaat, dan kesiapan teknologi organisasi merupakan variabel penting dalam penerapan sistem manajemen untuk manajemen risiko dan keamanan.

4. Kesimpulan

Kesimpulannya, penerapan Sistem Informasi Manajemen (SIM) terbukti memiliki peran krusial dalam meningkatkan efektivitas manajemen risiko dan keamanan informasi di dalam organisasi. Dengan adanya SIM yang terstruktur dan terintegrasi, organisasi mampu melakukan identifikasi, analisis, dan mitigasi risiko secara lebih cepat dan akurat. SIM memberikan akses data secara real- time, meningkatkan pengawasan, serta mendukung pengambilan keputusan yang tepat dalam mengelola ancaman terhadap keamanan informasi.

Namun keberhasilan penerapan SIM bergantung pada beberapa faktor, termasuk kesiapan teknologi, kompetensi sumber daya manusia, serta dukungan manajemen. Tantangan seperti resistensi terhadap perubahan dan keterbatasan anggaran juga perlu diatasi melalui pelatihan dan penerapan strategi pengembangan yang matang.

Oleh karena itu, SIM bukan hanya sekedar alat operasional, tetapi juga merupakan komponen strategi dalam menghadapi risiko dan menjaga keamanan informasi. Organisasi yang mampu memanfaatkan SIM secara optimal akan memiliki keunggulan kompetitif dalam menjaga ekosistem bisnis mereka di era digital yang penuh dengan tantangan keamanan.

Daftar Pustaka

Boehm, BW (2011). *Manajemen Risiko Perangkat Lunak: Prinsip dan Praktik.* PerangkatLunak IEEE, 8(1), 32-41.

Chen, H., Chiang, RHL, & Storey, VC (2012). *Kecerdasan Bisnis dan Analisis: Dari DataBesar hingga Dampak Besar.* MIS Quarterly, 36(4), 1165-1188.

Davis, FD (1989). *Kegunaan yang Dirasakan, Kemudahan Penggunaan yang Dirasakan, dan Penerimaan Pengguna terhadap Teknologi Informasi.* MIS Quarterly, 13(3), 319-340.

Dhillon, G., & Backhouse, J. (2001). *Arah Penelitian Keamanan Sistem Informasi Saat Ini:Menuju Perspektif Sosial-Organisasi.* Jurnal Sistem Informasi, 11(2), 127-153.

ISO 31000:2018. (2018). *Manajemen Risiko – Pedoman.* Organisasi Internasional untuk Standardisasi.

Laudon, KC, & Laudon, JP (2014). *Sistem Informasi Manajemen: Mengelola PerusahaanDigital* (edisi ke-13). Pearson.

McFarlan, FW, & Nolan, RL (2003). *Mengelola Risiko TI dalam Ekonomi Baru.* Harvard Business Review, 81(10), 86-94.

MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

O'Brien, JA, & Marakas, GM (2010). *Pengantar Sistem Informasi.* McGraw-Hill.

Rogers, EM (2003). *Difusi Inovasi* (edisi ke-5). Free Press.

Turban, E., Leidner, D., McLean, E., & Wetherbe, J. (2008). *Teknologi Informasi untuk Manajemen: Transformasi Organisasi dalam Ekonomi Digital*. John Wiley & Sons.

Whitman, ME, & Mattord, HJ (2012). *Prinsip Keamanan Informasi* (edisi ke-4). Cengage Learning