

Dampak Faktor Manusia dan Pengoptimalisasian Terhadap Integritas Data Perusahaan Dalam Lingkungan Bisnis

Dhea Putri Adhelia, Muhammad Irwan Padli Nasution

Universitas Islam Negeri Sumatera Utara

ARTICLE INFO

Article history:

Received June 15, 2025

Revised June 17, 2025

Accepted June 20, 2025

Available online June 25, 2025

Keywords

Data integrity; Business; Human Factors; Companies



This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.
Copyright © 2025 by Author. Published by Yayasan Daarul Huda

ABSTRACT

Integritas data adalah elemen yang sangat penting dalam lingkungan bisnis, karena berdampak pada proses pengambilan keputusan dan keberhasilan operasional. Salah satu penyebab utama yang memengaruhi integritas data adalah faktor manusia, yang meliputi kesalahan individu, perilaku, dan etika kerja. Penelitian ini bertujuan untuk mengevaluasi dampak faktor manusia terhadap integritas data dalam konteks bisnis, serta menggali strategi untuk mengurangi resiko yang mungkin muncul. Dengan menggunakan pendekatan kualitatif, mengidentifikasi berbagai cara dimana kesalahan dan perilaku manusia dapat mengancam akurasi dan keandalan data, serta memberikan rekomendasi untuk meningkatkan kesadaran dan pelatihan di kalangan staf

ABSTRACT

Data integrity is a crucial element in the business environment, as it impacts the decision-making process and operational success. One of the main causes affecting data integrity is human factors, which include individual errors, behavior, and work ethic. The research aims to evaluate the impact of human factors on data integrity in a business context, as well as dig into strategies to mitigate risks that may arise. Using a qualitative approach, identify various ways in which human error and behavior can threaten data accuracy and reliability, as well as provide recommendations for increased awareness and training among staff processes

PENDAHULUAN

Dalam era bisnis yang semakin mengandalkan data, integritas data menjadi salah satu fondasi penting yang memengaruhi keberhasilan operasional dan pengambilan keputusan strategis. Data yang tepat dan konsisten tidak hanya mendukung analisis yang akurat, tetapi juga membangun kepercayaan diantara pemangku kepentingan, yaitu pelanggan, investor, dan mitra bisnis. Meskipun teknologi dan sistem informasi terus berkembang, tantangan utama dalam menjaga integritas data tetaplah berasal dari faktor manusia.

Kesalahan yang dilakukan oleh individu, baik secara sengaja maupun tidak, sering kali menyebabkan data menjadi hilang dan tidak akurat, hilangnya informasi, atau bahkan kebocoran data yang sensitive. Yaitu seperti kesalahan dalam memasukkan data, pengabaian prosedur yang telah ditetapkan, dan kurangnya pelatihan yang memadai, semua ini dapat berkontribusi pada ketidakakuratan informasi. Pentingnya memahami bagaimana faktor manusia memengaruhi integritas data tidak bisa diabaikan. Banyak organisasi yang gagal mengelola aspek ini menghadapi konsekuensi serius, yaitu seperti kerugian finansial, kerusakan reputasi, dan hilangnya kepercayaan pelanggan.

Oleh karena itu, penelitian ini bertujuan untuk memberikan analisis mengenai berbagai jenis kesalahan yang mungkin terjadi, perilaku yang berkontribusi pada permasalahan yang ada, serta strategi efektif untuk meningkatkan kesadaran dan keterampilan karyawan dalam pengelolaan data.

METODE

Penelitian ini menggunakan studi kualitatif atau studi literatur, dimana sumber yang digunakan merupakan kumpulan dari artikel ilmiah yang terakreditasi yang membahas mengenai dampak faktor manusia dan pengoptimalisasian terhadap integritas data perusahaan dalam lingkungan bisnis.

HASIL DAN PEMBAHASAN

Integritas data merupakan elemen yang krusial dalam pengelolaan bisnis yang sukses. Data yang tepat dan konsisten sangat diperlukan untuk mendukung pengambilan keputusan yang akurat dan strategis. Namun, faktor manusia sering kali menjadi penyebab utama gangguan terhadap integritas data.

*Corresponding AAuthor

Email: dheaputri308@gmail.com, irwannst@uinsu.ac.id

Kesalahan dalam memasukkan data, ketidakpatuhan terhadap prosedur yang telah ditentukan, serta kurangnya pemahaman mengenai pentingnya pengelolaan data dapat mengakibatkan data yang tidak akurat.

Kurangnya kesadaran karyawan akan pentingnya keamanan data dapat membuka pintu bagi serangan siber, seperti *Phishing* atau *Malware*. Akses yang tidak sah ke data sensitif, baik disengaja maupun tidak, dapat mengakibatkan kebocoran informasi yang pada akhirnya dapat merugikan perusahaan.

Tidak hanya itu, integritas data juga dapat terancam oleh tindakan internal yang disengaja. Manipulasi data oleh karyawan untuk keuntungan pribadi atau untuk menutupi kesalahan dapat merusak keakuratan dan keandalan informasi bisnis. Tekanan dari manajemen untuk mencapai target kinerja tertentu juga dapat mendorong karyawan untuk melakukan praktik-praktik yang tidak etis yang membahayakan integritas data.

Langkah awal dalam menjaga integritas data adalah dengan menetapkan kebijakan dan prosedur keamanan yang jelas, kebijakan yang dirancang dengan baik memberikan panduan yang konkret bagi karyawan tentang cara menangani data. Kebijakan ini perlu dikomunikasikan dengan efektif agar semua karyawan memahami tanggung jawab mereka dalam menjaga keakuratan dan kerahasiaan data.

Pelatihan bagi karyawan juga merupakan bagian penting dalam meningkatkan kesadaran dan keterampilan mereka dalam pengelolaan data. Program pelatihan yang rutin dan efektif dapat membantu karyawan memahami prosedur yang benar serta risiko yang mungkin timbul jika data tidak dikelola dengan baik. Materi pelatihan harus mencakup topik seperti pengenalan terhadap keamanan data, cara mengidentifikasi potensi kesalahan, dan prosedur untuk melaporkan masalah. Dengan peningkatan keterampilan dan pengetahuan, karyawan akan lebih mampu menghindari kesalahan yang dapat merusak integritas data.

Teknologi informasi berperan penting dalam pengelolaan dan pemrosesan data secara efisien. Namun, tanpa adanya sistem keamanan yang memadai, kemajuan teknologi dapat membuka peluang bagi ancaman siber. Oleh karena itu, penting bagi manajemen untuk menerapkan teknologi yang tidak hanya berfungsi dengan baik tetapi juga dilengkapi dengan kontrol keamanan seperti otentikasi, enkripsi, dan manajemen akses. Selain itu, integrasi antara perangkat keras, perangkat lunak, dan prosedur operasional harus dirancang dengan cermat agar sistem informasi dapat berfungsi secara efektif sekaligus terlindungi dari gangguan.

Jaringan juga sangat penting dalam menjaga keamanan sistem informasi. Jaringan yang digunakan untuk komunikasi data antar perangkat harus dilindungi dari potensi penyusupan, penyadapan, atau serangan. Pengamanan jaringan mencakup perlindungan fisik dan logis, seperti penggunaan firewall, pengawasan akses, serta kebijakan penggunaan jaringan yang jelas.

Adapun tiga elemen penting dalam keamanan informasi yang saling terkait, yaitu CIA. Ini mencakup Confidentiality, Integrity, dan Availability. Confidentiality atau kerahasiaan sangat penting untuk memastikan bahwa hanya pihak-pihak yang berwenang yang dapat mengakses informasi. Dengan menerapkan kebijakan kontrol akses, enkripsi data, dan meningkatkan kesadaran akan risiko kebocoran informasi, perusahaan dapat mencegah akses tidak sah terhadap data sensitive. Hal ini juga berpengaruh pada kepercayaan pelanggan, karena mereka akan merasa lebih aman jika data mereka dikelola dengan baik dan terlindungi dari penyalahgunaan.

Integrity atau keutuhan data, berfungsi untuk memastikan bahwa informasi tetap tidak berubah, tidak dimanipulasi, atau tidak rusak, baik sengaja maupun tidak. Keberhasilan dalam menjaga integritas data sangat bergantung pada penerapan prosedur audit, penggunaan tanda tangan digital, dan sistem pelaporan otomatis yang dapat mendeteksi perubahan data yang mencurigakan. Apabila sebuah organisasi gagal menjamin integritas data, keputusan yang diambil berdasarkan informasi tersebut bisa jadi salah dan berpotensi merugikan operasional bisnis.

Availability atau ketersediaan, berkaitan dengan kemampuan sistem informasi untuk menyediakan data dan layanan yang kapan saja dibutuhkan oleh pihak yang berhak. Hal ini mencakup penerapan sistem cadangan (backup), pemulihan bencana (disaster recovery), pengelolaan kapasitas sistem, serta pemeliharaan infrastruktur teknologi informasi yang handal. Jika ketersediaan informasi terganggu, hal ini dapat menghambat kelangsungan operasional dan mengurangi efisiensi perusahaan.

SIMPULAN

Integritas data merupakan elemen penting dalam kelangsungan operasional sebuah bisnis, yang sangat dipengaruhi oleh faktor manusia. Kesalahan yang dilakukan oleh individu, ketidakpatuhan terhadap prosedur yang ada, serta perilaku tidak etis dapat membahayakan kurasi dan keandalan data. Untuk menjaga integritas data, perusahaan perlu menetapkan kebijakan dan prosedur keamanan yang jelas serta melakukan komunikasi efektif mengenai tanggung jawab setiap karyawan.

Pelatihan berkala bagi karyawan sangat diperlukan untuk meningkatkan kesadaran dan kemampuan mereka dalam pengelolaan data. Selain itu, penerapan teknologi informasi yang aman, seperti kontrol akses dan enkripsi, juga harus dilakukan untuk melindungi data dari potensi ancaman siber. Keamanan informasi bergantung pada tiga elemen utama, yaitu Kerahasiaan, Keutuhan, dan Ketersediaan (CIA). Memastikan kerahasiaan, integritas, dan aksesibilitas data akan membantu perusahaan dalam mencegah akses yang tidak sah dan menjaga kepercayaan pelanggan. Dengan langkah-langkah ini, perusahaan dapat mengurangi resiko yang berhubungan dengan faktor manusia dan memastikan integritas data tetap terjaga, yang pada gilirannya mendukung keputusan yang strategis.

REFERENSI

- Bariqi, M. D. (2018). Pelatihan dan pengembangan sumber daya manusia. *Jurnal Studi Manajemen dan Bisnis*, 5(2).
- Budi, D. S., & Tarigan, A. (2018). Konsep dan Strategi Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI). *Jurnal Sistem Informasi Bisnis*, 2(1).
- Budiarto, D. S., Fachrunnisa, Z. H., Pramudiati, N., Putri, A. Z., & Hidayat, M. A. N. (2023). Pentingnya integritas untuk mengurangi kecurangan akuntansi pada perusahaan. *UBMJ (UPY Business and Management Journal)*, 2(2), 1–9.
- Eliza, Y. (2015). Pengaruh Moralitas Individu Dan Pengendalian Internal Terhadap Kecenderungan Kecurangan Akuntansi. *Jurnal Akuntansi*, 4(2), 86–100.
- Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-faktor yang mempengaruhi keamanan sistem informasi: Keamanan informasi, teknologi informasi dan network (Literature Review SIM). *Jurnal Ekonomi Manajemen Sistem Informasi (JEMSI)*, 3(5), 564–573.
- Puriwigati, A. N., & Buana, U. M. (2020). Sistem Informasi Manajemen-Kepuasan Informasi. *May*.
- Vansuri, R., Fauzi, A., Prasetyo, E. T., Negara, R., Ramadhan, R., Restu, A. M., & Firmansyah, R. R. (2023). Peran CIA (Confidentiality, Integrity, Availability) terhadap manajemen keamanan informasi. *Jurnal Ilmu Multidisiplin (JIM)*, 2(1), 106–113.
- Yuliana, A. (2016). Pengaruh Keadilan Organisasi, Sistem Pengendalian Intern Dan Komitmen Organisasi Terhadap Kecurangan (Fraud). *JOM Fekon*, 3(1).
- Zhang, Y., Man, H., Liang, J., & Su, Y. (2018). The role of training and security awareness in information security management: a literature review. *Journal of Computer Information Systems*, 58(1), 1-10.