

ANALISIS RISIKO DALAM AUDIT SISTEM INFORMASI STMIK KAPUTAMA BINJAI

Bremando Sibero¹, Regiba Fihl Adamsyah², Yuni Mahdalena³, Wanda Arfilla Daulay⁴

^{1,2,3,4}Jurusan sistem informasi, STMIK kaputama

Email: bremandosibero@gmail.com¹, regibaadamsyah5@gmail.com²,
yunimahdalena062004@gmail.com³, wandaarfilla988@gmail.com⁴

ABSTRAK – Penelitian ini bertujuan untuk menganalisis risiko dalam audit sistem informasi di STMIK Kaputama Binjai. Tujuan utama dari penelitian ini adalah untuk mengidentifikasi dan mengevaluasi berbagai risiko yang dapat mempengaruhi efektivitas dan keandalan sistem informasi di lembaga tersebut. Metode yang digunakan dalam penelitian ini adalah pendekatan kualitatif dengan pengumpulan data melalui wawancara, observasi, dan dokumentasi. Hasil penelitian menunjukkan bahwa terdapat beberapa risiko yang berpotensi mengganggu kinerja sistem informasi, seperti kelemahan dalam pengendalian akses, kurangnya pembaruan perangkat keras dan perangkat lunak, serta ketergantungan yang tinggi terhadap sistem tertentu. Penelitian ini juga mengidentifikasi pentingnya penerapan prosedur audit yang lebih ketat dan penggunaan teknologi yang lebih canggih untuk memitigasi risiko yang ada. Simpulan dari penelitian ini adalah bahwa risiko dalam audit sistem informasi di STMIK Kaputama Binjai perlu dikelola dengan baik melalui peningkatan pengendalian internal dan evaluasi sistem secara berkala untuk memastikan keberlanjutan dan keandalan sistem informasi di masa depan.

Kata Kunci: Risiko, Audit, Sistem Informasi, Pengendalian Internal, STMIK Kaputama Binjai

ABSTRACT - This research aims to analyze the risks in auditing information systems at STMIK Kaputama Binjai. The main objective of this research is to identify and evaluate various risks that can affect the effectiveness and reliability of information systems at the institution. The method used in this research is a qualitative approach with data collection through interviews, observation, and documentation. The results showed that there were several risks that could potentially disrupt the performance of information systems, such as weaknesses in access control, lack of hardware and software updates, and high dependence on certain systems. This study also identified the importance of implementing stricter audit procedures and the use of more sophisticated technology to mitigate existing risks. The conclusion of this study is that risks in information system audits at STMIK Kaputama Binjai need to be managed properly through improved internal controls and periodic system evaluations to ensure the sustainability and reliability of information systems in the future.

Keywords: Risk, Audit, Information System, Internal Control, STMIK Kaputama Binjai

PENDAHULUAN

Perkembangan teknologi informasi yang pesat saat ini membawa dampak signifikan terhadap hampir semua sektor kehidupan, termasuk di bidang pendidikan. Sistem informasi digunakan untuk mendukung berbagai proses operasional dan pengambilan keputusan yang lebih efektif. Namun, seiring dengan meningkatnya ketergantungan terhadap teknologi, risiko yang berkaitan dengan sistem informasi juga semakin kompleks. Risiko-risiko tersebut dapat mencakup gangguan operasional, kerugian finansial, hingga ancaman terhadap keamanan data. Oleh karena itu, penting bagi institusi pendidikan, seperti STMIK Kaputama Binjai, untuk melakukan audit terhadap sistem informasi yang digunakan guna mengidentifikasi dan mengelola risiko-risiko yang mungkin timbul.

Dalam konteks ini, audit sistem informasi berfungsi sebagai sarana untuk menilai keandalan dan efektivitas sistem informasi, serta untuk memastikan bahwa sistem tersebut dapat mendukung pencapaian tujuan organisasi dengan baik. Namun, proses audit seringkali dihadapkan pada tantangan, seperti ketidaktahuan mengenai potensi risiko yang ada dan kurangnya pengetahuan dalam penanganan masalah-masalah teknis yang terkait dengan sistem informasi. Oleh karena itu, penelitian ini bertujuan untuk menganalisis berbagai risiko yang ada dalam audit sistem informasi di STMIK Kaputama Binjai, serta memberikan rekomendasi untuk meningkatkan pengelolaan risiko di masa depan.

Tujuan utama dari penelitian ini adalah untuk mengidentifikasi dan mengevaluasi risiko yang dapat mempengaruhi kinerja sistem informasi di

STMIK Kaputama Binjai, serta untuk memberikan pemahaman yang lebih mendalam tentang pentingnya pengendalian risiko dalam sistem informasi. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan terhadap peningkatan kualitas sistem informasi di lembaga pendidikan tersebut, serta memberikan wawasan bagi pengelola sistem informasi dalam menghadapi berbagai tantangan yang ada.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif untuk menganalisis risiko dalam audit sistem informasi di STMIK Kaputama Binjai. Subjek penelitian adalah sistem informasi yang digunakan oleh lembaga tersebut, yang meliputi perangkat keras, perangkat lunak, dan prosedur operasional yang ada. Teknik pengumpulan data dilakukan melalui wawancara mendalam dengan pihak-pihak yang terkait langsung dengan pengelolaan dan penggunaan sistem informasi, seperti staf IT, pengguna sistem, dan manajer. Selain itu, data juga dikumpulkan melalui observasi terhadap proses operasional yang berkaitan dengan penggunaan sistem informasi dan dokumentasi terkait.

Desain penelitian ini adalah studi kasus, yang bertujuan untuk menggali secara mendalam masalah yang dihadapi oleh STMIK Kaputama Binjai dalam pengelolaan risiko sistem informasi. Teknik analisis data yang digunakan adalah analisis tematik, di mana data yang diperoleh dari wawancara dan observasi akan dianalisis untuk mengidentifikasi pola dan tema yang berkaitan dengan risiko sistem informasi. Penelitian ini tidak menggunakan model statistik karena berfokus pada pemahaman kualitatif mengenai risiko-risiko yang ada.

observasi terhadap proses operasional yang berkaitan dengan penggunaan sistem informasi dan dokumentasi terkait.

Desain penelitian ini adalah studi kasus, yang bertujuan untuk menggali secara mendalam masalah yang dihadapi oleh STMIK Kaputama Binjai dalam pengelolaan risiko sistem informasi. Teknik analisis data yang digunakan adalah analisis tematik, di mana data yang diperoleh dari wawancara dan observasi akan dianalisis untuk mengidentifikasi pola dan tema yang berkaitan dengan risiko sistem informasi. Penelitian ini tidak menggunakan model statistik karena berfokus pada pemahaman kualitatif mengenai risiko-risiko yang ada.

HASIL DAN PEMBAHASAN

Berdasarkan hasil penelitian yang dilakukan di STMIK Kaputama Binjai, terdapat berbagai risiko yang memengaruhi kinerja dan keberlanjutan sistem informasi di lembaga ini. Berdasarkan analisis data dari wawancara, observasi, dan dokumentasi, risiko-risiko tersebut dapat dikelompokkan menjadi tiga kategori utama: risiko keamanan, risiko operasional, dan risiko teknis.

A. Risiko Keamanan

Risiko keamanan menjadi salah satu perhatian utama dalam audit sistem informasi di STMIK Kaputama Binjai. Berdasarkan hasil wawancara dengan staf IT dan pengguna sistem, ditemukan bahwa masih terdapat beberapa celah yang berpotensi mengancam integritas dan kerahasiaan data yang dikelola oleh sistem informasi. Salah satu masalah utama adalah pengelolaan akses pengguna yang belum optimal. Penggunaan password yang kurang kuat dan praktik pengelolaan

hak akses yang tidak sesuai dengan peran masing-masing pengguna menjadi faktor yang meningkatkan potensi risiko terhadap keamanan sistem. Misalnya, beberapa pengguna memiliki akses ke data sensitif atau fitur sistem yang tidak diperlukan untuk pekerjaan mereka, yang memperbesar kemungkinan akses tidak sah atau penyalahgunaan informasi.

B. Risiko Operasional

Selain risiko keamanan, penelitian ini juga mengidentifikasi risiko operasional yang berkaitan dengan kelancaran proses bisnis yang mendukung operasional STMIK Kaputama Binjai. Berdasarkan hasil observasi terhadap penggunaan sistem informasi yang ada, ditemukan bahwa sering kali terjadi gangguan dalam sistem yang menghambat kelancaran berbagai proses administrasi penting. Salah satu contohnya adalah keterlambatan dalam pendaftaran mahasiswa baru, pengelolaan data akademik, serta pelaporan kegiatan administrasi lainnya. Gangguan ini mempengaruhi efisiensi operasional lembaga, karena dapat menimbulkan antrian atau keterlambatan dalam pelayanan kepada mahasiswa dan staf pengajar.

C. Risiko Teknis

Risiko teknis juga menjadi faktor penting yang perlu mendapatkan perhatian serius dalam audit sistem informasi di STMIK Kaputama Binjai. Hasil wawancara dengan staf IT mengungkapkan bahwa beberapa perangkat keras dan perangkat lunak yang digunakan di lingkungan kampus sudah usang dan tidak lagi mampu mendukung kebutuhan operasional yang terus berkembang. Beberapa sistem utama yang digunakan untuk proses administrasi dan akademik,

seperti sistem pendaftaran mahasiswa, manajemen nilai, dan pengelolaan data akademik, mengandalkan perangkat keras dan perangkat lunak yang sudah tidak diperbarui dalam waktu yang lama. Akibatnya, sistem-sistem ini mengalami keterbatasan dalam hal performa dan kemampuan untuk mengatasi kebutuhan

SIMPULAN

Berdasarkan hasil penelitian tentang analisis risiko dalam audit sistem informasi di STMIK Kaputama Binjai, dapat disimpulkan bahwa terdapat tiga jenis risiko utama yang dapat mempengaruhi operasional dan keamanan sistem informasi di lembaga ini, yaitu risiko keamanan, risiko operasional, dan risiko teknis. Risiko keamanan terkait dengan pengelolaan akses sistem yang kurang ketat, sementara risiko operasional lebih berkaitan dengan gangguan teknis yang disebabkan oleh perangkat keras dan perangkat lunak yang sudah usang. Adapun risiko teknis lebih berfokus pada ketergantungan terhadap perangkat yang tidak dapat lagi mendukung kebutuhan operasional yang semakin berkembang. Penelitian ini juga menemukan bahwa STMIK Kaputama Binjai belum memiliki kebijakan pengelolaan risiko yang terpadu dan terstruktur, sehingga pengelolaan risiko yang ada masih bersifat reaktif.

Untuk mengatasi berbagai risiko ini, penelitian ini merekomendasikan agar STMIK Kaputama Binjai mengembangkan kebijakan pengelolaan risiko yang lebih terstruktur, memperkuat pengawasan akses sistem, melakukan pembaruan sistem secara rutin, serta memberikan pelatihan kepada staf untuk meningkatkan efisiensi dan keamanan penggunaan sistem. Selain itu, perlu dilakukan investasi dalam perangkat keras dan perangkat lunak yang lebih baru

serta perbaikan sistem backup dan pemulihan data. Penerapan kebijakan pengelolaan risiko yang lebih baik diharapkan dapat meningkatkan keandalan dan efektivitas sistem informasi, sekaligus mendukung keberlanjutan operasional STMIK Kaputama Binjai di masa depan.

DAFTAR PUSTAKA

- Agustin, D., & Sari, Y. (2022). Manajemen Risiko dalam Sistem Informasi: Perspektif Keamanan dan Operasional. *Jurnal Teknologi Informasi*, 19(1), 23-34.
- Anderson, C., & Williams, P. (2020). Evaluating Information System Risks in Higher Education. *International Journal of Computer Science and Education*, 18(3), 143-156.
- Fitriani, L., & Ramadhani, A. (2021). Strategi Pengelolaan Risiko Teknologi Informasi pada Lembaga Pendidikan. *Jurnal Sistem Informasi*, 11(4), 82-96.
- Kurniawan, D., & Hidayati, N. (2020). Penerapan Kebijakan Pengelolaan Risiko pada Sistem Informasi di Perguruan Tinggi. *Jurnal Ilmiah Teknologi dan Manajemen*, 15(2), 67-75.
- Rahman, M., & Setiawan, T. (2021). Pendekatan Proaktif dalam Pengelolaan Risiko Keamanan Informasi. *Jurnal Keamanan Siber*, 8(2), 99-110.
- Smith, J., & Brown, L. (2022). Mitigating Technical Risks in Information Systems: Best Practices and Challenges. *Journal of Information Technology and Security*, 24(2), 201- 215.
- Williams, R. (2019). Information Technology and Risk Management in Academic Institutions. *Journal of Risk Assessment and Management*, 22(1), 50-62.
- Zhang, X., & Chen, H. (2020). The Impact of Obsolete Hardware and Software on Operational Risks in Educational Institutions. *Journal of Educational Systems and Technology*, 14(3), 115-128.