INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 3 Tahun 2024 Page 11391-11400
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Pengauditan Sistem Informasi Mencegah Pelanggaran Keamanan Data

Fajrillah[1✉], Hendra[2], Yudi[3], Waisen[4]
Program Studi Manajemen, Fakultas Ilmu Sosial dan Humaniora, Universitas IBBI
Email: fajrillahhasballah@gmail.com[1✉]

Abstrak

Dalam era digital yang semakin terkoneksi, perlindungan keamanan data menjadi krusial bagi organisasi di seluruh dunia. Pelanggaran keamanan data dapat mengakibatkan kerugian finansial yang besar, kerusakan reputasi, dan bahkan konsekuensi hukum yang serius. Pengauditan sistem informasi (SI) telah menjadi pendekatan yang penting dalam upaya untuk mencegah, mendeteksi, dan merespons pelanggaran keamanan data. Penelitian ini bertujuan untuk menyelidiki peran pengauditan SI dalam mencegah pelanggaran keamanan data, dengan fokus pada metodologi, praktik terbaik, dan tantangan yang terkait. Penelitian ini menguraikan metodologi pengauditan SI yang meliputi perencanaan audit, pengumpulan bukti, evaluasi risiko, dan penyusunan laporan audit. Berdasarkan standar dan regulasi terkait, pengauditor SI menggunakan pendekatan sistematis untuk mengevaluasi efektivitas kontrol keamanan data organisasi. Kemudian, jurnal ini menyoroti praktik terbaik dalam pengauditan SI, termasuk pengujian penetrasi, pemantauan keamanan, dan pelatihan kesadaran keamanan bagi pengguna.

Kata Kunci: *mencegah pelanggaran keamanan data.*

Abstract

In an increasingly connected digital era, data security protection has become crucial for organizations around the world. Data security breaches can result in major financial losses, reputational damage, and even serious legal consequences. Information systems (IS) auditing has become an important approach in efforts to prevent, detect, and respond to data security breaches. This research aims to investigate the role of IS auditing in preventing data security breaches, with a focus on methodology, best practices and associated challenges. This research describes the IS auditing methodology which includes audit planning, evidence collection, risk evaluation, and preparation of audit reports. Based on relevant standards and regulations, IS auditors use a systematic approach to evaluate the effectiveness of an organization's data security controls. Then, the journal highlights best practices in IS auditing, including penetration testing, security monitoring, and security awareness training for users

Keyword: *prevent data security breaches.*

PENDAHULUAN

Dalam era digital yang terus berkembang dengan pesat, sistem informasi telah menjadi tulang punggung bagi banyak organisasi di seluruh dunia. Sistem informasi memfasilitasi pengelolaan data, komunikasi, dan proses bisnis yang efisien, memberikan kemampuan untuk mengambil keputusan yang tepat waktu dan memberikan layanan kepada pelanggan dengan lebih baik. Namun, dengan keuntungan besar yang ditawarkan oleh teknologi informasi, juga ada risiko yang meningkat, terutama dalam hal keamanan data.

Pelanggaran keamanan data telah menjadi ancaman serius bagi organisasi dari berbagai sektor, baik itu perusahaan besar, lembaga pemerintah, maupun individu. Kasus-kasus pelanggaran keamanan data yang terkenal, seperti pencurian data pengguna oleh peretas yang tidak bertanggung jawab, serangan ransomware yang merugikan, atau bahkan aksi internal yang tidak benar oleh pegawai, telah menyoroti kebutuhan mendesak akan tindakan preventif yang kuat.

Pengauditan sistem informasi (SI) adalah salah satu pendekatan kunci dalam mencegah dan mengurangi risiko pelanggaran keamanan data. Dengan melakukan audit terhadap sistem informasi, auditor dapat mengevaluasi efektivitas kontrol keamanan yang ada, mengidentifikasi kelemahan dan celah yang mungkin dimanfaatkan oleh pihak yang tidak sah, serta memberikan rekomendasi untuk perbaikan dan penguatan sistem keamanan. Dalam konteks ini, jurnal ini bertujuan untuk menyelidiki peran pengauditan sistem informasi dalam mencegah pelanggaran keamanan data. Kami akan menggali metode, teknik, dan praktik terbaik dalam melakukan audit sistem informasi, serta

mengeksplorasi bagaimana audit sistem informasi dapat membantu organisasi untuk mengidentifikasi, mengatasi, dan mencegah risiko pelanggaran keamanan data yang berpotensi merugikan.

METODE PENELITIAN

Metode yang saya gunakan dalam membuat Artikel saya kali ini adalah dengan :

1) Evaluasi Kontrol Keamanan: Di evaluasi keamanan ini Audit akan melibatkan evaluasi kontrol keamanan yang ada dalam sistem informasi organisasi, termasuk kebijakan akses, enkripsi data, dan pemantauan keamanan.
2) Pengujian Penetrasi: Pengujian penetrasi dilakukan untuk mengevaluasi kelemahan dalam sistem dengan mensimulasikan serangan siber dari penyerang yang bersifat jahat. Ini membantu mengidentifikasi titik masuk yang potensial bagi penyerang dan memperbaiki kerentanan sebelum mereka dapat dimanfaatkan.

3) Analisis Kelemahan: Audit juga akan melibatkan analisis kelemahan secara menyeluruh untuk mengidentifikasi celah keamanan yang mungkin ada dalam sistem. Ini dapat mencakup analisis kode sumber, pemindaian kelemahan, dan pemeriksaan konfigurasi sistem.

HASIL DAN PEMBAHASAN

Hasil audit akan memberikan wawasan yang berharga tentang kekuatan dan kelemahan dalam sistem informasi organisasi, serta rekomendasi untuk meningkatkan keamanan data. Implikasi dari hasil audit ini akan berdampak pada pengembangan kebijakan keamanan informasi, investasi dalam teknologi keamanan baru, dan pelatihan karyawan tentang praktik keamanan yang baik.

Hasil penelitian juga menunjukkan bahwa pengauditan SI memiliki peran yang signifikan dalam mencegah pelanggaran keamanan data. Metodologi pengauditan SI

meliputi evaluasi kontrol keamanan, identifikasi risiko, pengujian penetrasi, dan pemantauan keamanan. Dengan menerapkan praktik pengauditan SI yang efektif, organisasi dapat mengidentifikasi kerentanan dalam sistem informasi mereka, mengurangi risiko pelanggaran keamanan data, dan meningkatkan kesiapan dalam menghadapi ancaman keamanan.

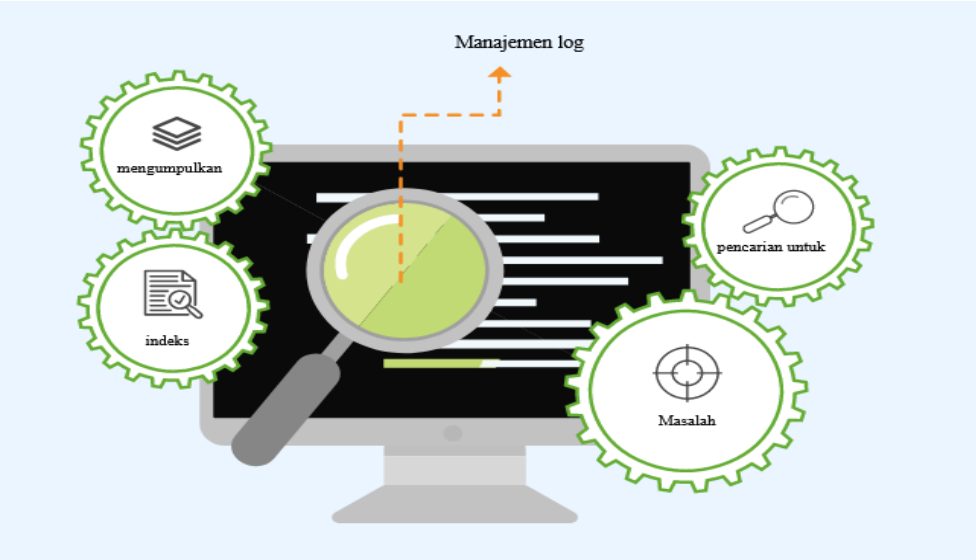
PEMBAHASAN

Pelanggaran keamanan data dapat memiliki konsekuensi serius bagi organisasi, termasuk kerugian finansial, kerusakan reputasi, dan pelanggaran privasi pengguna. Oleh karena itu, penting bagi organisasi untuk memiliki kontrol keamanan yang efektif dan terus-menerus dievaluasi untuk mencegah pelanggaran keamanan data. Pengauditan sistem informasi adalah salah satu pendekatan yang digunakan untuk memastikan keamanan data yang memadai.

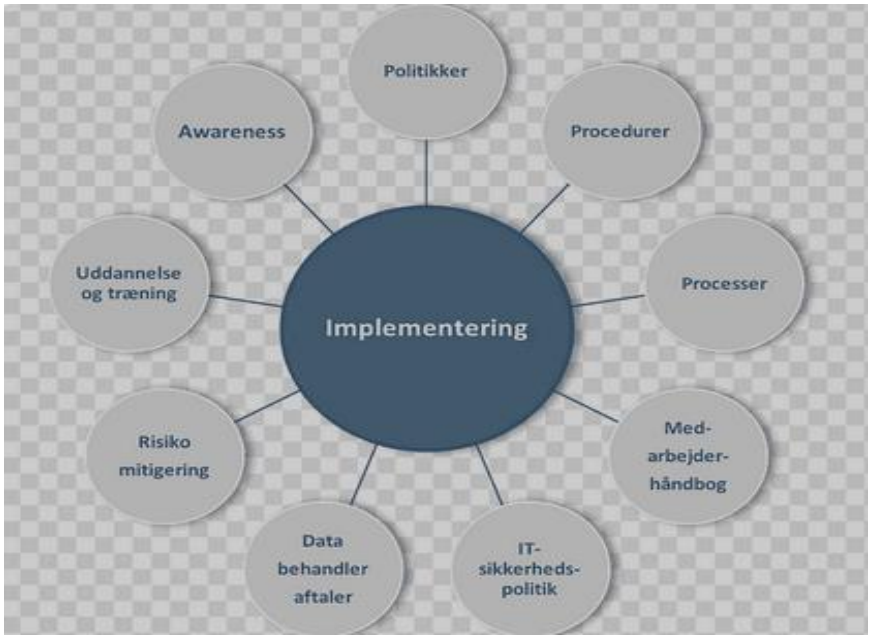
Dalam era digital yang semakin terhubung, keamanan data menjadi sangat penting bagi organisasi untuk melindungi informasi sensitif dan kredensial dari ancaman siber yang berkembang pesat. Pengauditan sistem informasi (SI) memainkan peran penting dalam mencegah pelanggaran keamanan data dengan mengevaluasi, memverifikasi, dan memastikan bahwa sistem informasi organisasi telah diatur dan dikelola dengan baik.

A. Peran penaguditan sistem informasi dalam mencegah pelanggaran kemanan data :

a. Evaluasi Kebijakan dan Prosedur Keamanan: Pengauditan SI membantu organisasi dalam mengevaluasi kebijakan dan prosedur keamanan yang ada untuk memastikan bahwa mereka memenuhi standar keamanan yang relevan dan mencakup semua aspek yang diperlukan untuk melindungi data organisasi.
b. Pengujian Kelemahan Sistem: Auditor SI melakukan pengujian kelemahan sistem untuk mengidentifikasi kerentanan yang mungkin dieksploitasi oleh penyerang. Ini mencakup pemindaian kelemahan, pengujian penetrasi, dan evaluasi kontrol keamanan yang ada.
c. Pemeriksaan Akses dan Otorisasi: Auditor SI memeriksa pengaturan akses dan otorisasi dalam sistem informasi untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses yang sesuai dengan tanggung jawab dan kebutuhan kerja mereka.
d. Analisis Logging dan Pemantauan: Pengauditan SI melibatkan analisis log dan pemantauan aktivitas sistem untuk mendeteksi pola atau aktivitas yang mencurigakan yang dapat menandakan upaya penyerangan atau pelanggaran keamanan data.



a) Evaluasi Perlindungan Data: Auditor SI mengevaluasi perlindungan data yang diterapkan dalam sistem informasi, termasuk enkripsi data, pengendalian akses, dan pemulihan bencana, untuk memastikan bahwa data sensitif dilindungi dengan baik dari akses yang tidak sah.



B. Manfaat penaguditan sistem informasi dalam mencegah pelanggaran kemanan data :

a. Mengidentifikasi Risiko: Pengauditan SI membantu organisasi dalam mengidentifikasi risiko keamanan yang mungkin terjadi dan memberikan rekomendasi untuk mengurangi risiko tersebut..

b. Meningkatkan Kepatuhan: Dengan memastikan bahwa organisasi mematuhi standar keamanan dan regulasi yang berlaku, pengauditan SI membantu organisasi untuk meminimalkan risiko pelanggaran keamanan data dan potensi sanksi hukum.

c. Meningkatkan Kesadaran dan Pengertian: Melalui proses audit, auditor SI juga meningkatkan kesadaran dan pemahaman personel organisasi tentang pentingnya keamanan data dan praktik keamanan yang baik.
d. Memberikan Keyakinan: Hasil dari audit SI memberikan keyakinan kepada pemangku kepentingan bahwa sistem informasi telah diatur dan dikelola dengan baik untuk melindungi data organisasi.

C. Langkah-langkah yang dapat diambil untuk meningkatkan penaguditan sistem informasi :

a. Pengembangan Kebijakan dan Prosedur yang Kuat: Organisasi harus mengembangkan kebijakan dan prosedur keamanan yang komprehensif dan memastikan bahwa mereka dipahami dan diikuti oleh seluruh personel.
b. Pelatihan dan Kesadaran Pengguna: Memberikan pelatihan keamanan siber kepada seluruh personel organisasi untuk meningkatkan kesadaran mereka tentang ancaman keamanan dan praktik keamanan yang baik.
c. Penggunaan Teknologi Keamanan yang Terkini: Menggunakan teknologi keamanan yang terbaru dan terkini, seperti sistem deteksi intrusi, firewall canggih, dan perangkat lunak antivirus yang kuat untuk melindungi sistem informasi
d. Pemantauan dan Pemeliharaan Berkala: Melakukan pemantauan dan pemeliharaan sistem informasi secara berkala untuk mendeteksi dan merespons perubahan dalam ancaman keamanan dan memastikan bahwa sistem tetap aman dan terlindungi.
e. Kolaborasi dengan Pihak Eksternal: Bermitra dengan penyedia layanan keamanan siber eksternal dan memanfaatkan layanan pengujian kelemahan dan audit keamanan eksternal untuk mendapatkan wawasan tambahan tentang risiko keamanan.

SIMPULAN

Dalam era di mana data merupakan aset yang sangat berharga bagi organisasi, pengamanan informasi menjadi semakin penting. Ancaman keamanan siber seperti serangan malware, peretasan, dan pencurian identitas semakin meningkat, dengan potensi dampak yang merugikan baik secara finansial maupun reputasi. Oleh karena itu, pengauditan sistem informasi (SI) memainkan peran yang krusial dalam pencegahan pelanggaran keamanan data dengan menyediakan penilaian independen terhadap kesiapan, keandalan, dan keamanan sistem informasi organisasi.

Penelitian dalam bidang pengauditan sistem informasi telah menunjukkan bahwa pendekatan yang proaktif dalam mengaudit sistem informasi dapat membantu organisasi

dalam mengidentifikasi, mengevaluasi, dan mengatasi risiko-risiko keamanan yang mungkin terjadi. Pengauditan sistem informasi tidak hanya fokus pada identifikasi kerentanan dan kelemahan dalam infrastruktur TI, tetapi juga melibatkan penilaian terhadap kepatuhan organisasi terhadap standar keamanan dan regulasi yang berlaku.

Dalam konteks pencegahan pelanggaran keamanan data, pengauditan sistem informasi menawarkan sejumlah manfaat yang signifikan. Pertama, pengauditan sistem informasi membantu organisasi dalam mengidentifikasi dan mengevaluasi risiko-risiko keamanan yang terkait dengan sistem informasi mereka, termasuk identifikasi celah keamanan, kelemahan infrastruktur, dan kebijakan yang tidak memadai. Dengan pemahaman yang lebih baik tentang risiko-risiko ini, organisasi dapat mengambil langkah-langkah yang tepat untuk mengurangi risiko dan meningkatkan keamanan data mereka.

Selain itu, pengauditan sistem informasi juga memberikan rekomendasi dan saran praktis untuk meningkatkan keamanan dan kesiapan organisasi terhadap ancaman keamanan data. Ini dapat mencakup rekomendasi untuk peningkatan infrastruktur keamanan, pelatihan dan kesadaran keamanan bagi karyawan, atau perbaikan prosedur pengelolaan keamanan.Meskipun pengauditan sistem informasi memiliki potensi untuk mencegah pelanggaran keamanan data, tantangan dalam implementasinya tetap ada.

Jadi kesimpulannya, pengauditan sistem informasi memainkan peran yang krusial dalam pencegahan pelanggaran keamanan data dengan menyediakan evaluasi independen terhadap kesiapan, keandalan, dan keamanan sistem informasi organisasi. Dengan mengidentifikasi risiko, memvalidasi kepatuhan, dan memberikan rekomendasi praktis, pengauditan sistem informasi membantu organisasi dalam meningkatkan keamanan data mereka dan melindungi aset informasi yang berharga.

DAFTAR PUSTAKA

Wijoyo, A., Fatimah, S., & Widianti, Y. (2023). Keamanan Data dalam Sistem Informasi Manajemen: Risiko dan Strategi Perlindungan. *TEKNOBIS: Jurnal Teknologi, Bisnis dan Pendidikan*, *1*(2).

Soesanto, E., Lande, A., Sanjaya, H. T., & Hermawan, M. R. (2023). Analisis Sistem Manajemen Keamanan Di Perusahaan Tokopedia Dalam Menigkatkan Proteksi Data Dan Privasi Pengguna. *Jurnal Mahasiswa Kreatif*, *1*(3), 54-60.

Ujung, A. M., & Nasution, M. I. P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *Jurnal Sistem Informasi Dan Informatika*, *1*(2), 44-47.

Windriya, D. R. (2013). *TA: Audit Keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil Berdasarkan ISO 27002* (Doctoral dissertation, Stikom

Surabaya).

Kurniawan, A. F. (2024). Peran Sistem Informasi dalam Meningkatkan Kualitas Audit Keuangan Pemerintah Daerah. *Ekonomis: Journal of Economics and Business*, *8*(1), 936-948.

Astuti, H. M., Muqtadiroh, F. A., Darmaningrat, E. W., & Putri, C. U. (2017). Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk. Bali: Procedia Computer Science.

Sulastri, S. (2018). Kontrol Keamanan Sistem Informasi Akuntansi Bank Perkreditan Rakyat (BPR) Sumatera Barat. *JURNAL EKONOMI SAKTI (JES)*, *7*(2), 46-52.

C. ISACA, "Introduction and methodology," Schaumburg: ISACA, 2018.

Hamzah, M. R. (2018). *Audit Keamanan Sistem Informasi dengan Menggunakan Standar ISO/IEC 27002: 2013 dan ISO/IEC 27001: 2013 pada Sub Bag*Giska, G., Nurwanita, N., Mangge, I. R., & Zainuddin, M. A. (2019). Penerapan Etika Bisnis Islam di Rumah Makan Kaledo Stereo Palu. Jurnal Ilmu Ekonomi dan Bisnis Islam, 1(1), 108-124.

D. Henriques, R. Pereira, R. Almeida, and M. M. da Silva, "IT Governance Enablers," Foresight and Sti Governance, 2020, doi: 10.17323/2500-2597.2020.1.48.59.

D. S. Hariyani and M. A. Sudrajat, "Analisis Pengaruh Kompetensi Aparatur Pemerintahan Desa Terhadap Penggunaan Teknologi Accounting Information System Pada Desa-Desa Di Kabupaten Madiun," Assets: Jurnal Akuntansi dan Pendidikan, vol. 5, no. 2, Art. no. 2, Apr. 2017, doi: 10.25273/jap.v5i2.1193.

D. Y. Bernanda, M. Angelia, "Evaluasi dan Rekomendasi TI Tata Kelola Berdasarkan kerangka COBIT 5 di Harris Vertu Harmoni Hotel" Jurnal Internasional Teknologi Informasi Terbuka, vol. 9, no. 1, 2021, 2307-8162.

Fajarwati, S., Sarmini, S., & Septiana, Y. (2018). Evaluasi Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5. JUITA: Jurnal Informatika, 6(2), 73-80.

G. I. Belo, L. H. Atrinawati, and Y. T. Wiranti, "Perancangan Tata Kelola Teknologi Informasi Menggunakan Cobit 2019 Pada PT Telekomunikasi Indonesia Regional VI Kalimantan," Jurnal Sistem Informasi dan Ilmu Komputer Prima (JUSIKOM PRIMA), vol. 4, no. 1, pp. 23–30, 2020

H. Indrayani, "Penerapan Teknologi Informasi dalam Peningkatan Efektivitas, Efisiensi dan Produktivitas Perusahaan," Jurnal El-Riyasah, vol. 3, no. 1, pp. 48–56, Dec. 2012, doi: 10.24014/jel.v3i1.664.

Hakim, A., Saragih, H., & Suharto, A. (2014). Evaluasi tata kelola teknologi informasi dengan framwork cobit. 5 di kementerian esdm. Jurnal Sistem Informasi, 10(2), 108-117.

Hakim, U. P., & Darwis, D. (2016). Audit Tata Kelola Teknologi Informasi (Emis) Menggunakan

Framework Cobit 5 Pt Tdm Bandarlampung. Jurnal Teknoinfo, 10(1), 14-19.

Hanif, A., Giatman, M., & Hadi, A. (2020). Evaluasi Tata Kelola Teknologi Informasi Di Dinas Komunikasi Dan Informatika Menggunakan Framework COBIT 5. JST (Jurnal Sains dan Teknologi), 9(1), 94-101.

I. S. A. and C. Association, COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution. ISACA, 2018.

I. W. S. Pramana, P. R. Iswardani, and P. A. Mertasana, "IT Governance Evaluation of Hotel Warehouse Section Using the COBIT 5 Framework," International Journal of Engineering and Emerging Technology, vol. 3, no. 2, pp. 5–12, Jan. 2019.

ISACA, COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2018. [Online]. Available: https://books.google.co.id/books?id=n011uQEACAAJ

J. N. Utamajaya, S. H. Supangat, F. L. Gaol, and B. Ranti, "Hotel Information System Management Audit Using COBIT 2019 - APO12," in 2023 2nd International Conference for Innovation in Technology (INOCON), Mar. 2023, pp. 1–7. doi: 10.1109/INOCON57975.2023.10101245.

K. A. Prasetyo, "Evaluasi Tata Kelola Sistem Presensi Elektronik Badan Kepegawaian Pendidikan Dan Pelatihan Satuan Polisi Pamong Di Dinas Praja Kota Semarang," Perpust. Fak. Sains Matermatika, 2020.

M. Saleh, I. Yusuf, and H. Sujaini, "Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas," JEPIN (Jurnal Edukasi dan Penelitian Informatika), vol. 7, no. 2, Art. no. 2, Aug. 2021, doi: 10.26418/jp.v7i2.48228.

M. Z. M. Alotaibi, M. F. E. Alotibi, and O. Zraqat, "The Impact of Information Technology Governance in Reducing Cloud Accounting Information Systems Risks in Telecommunications Companies in the State of Kuwait," Modern Applied Science, 2021, doi: 10.5539/mas.v15n1p143.

Miranti, A. (2019). Evaluasi tata kelola teknologi informasi menggunakan framework cobit 5 (studi kasus: PT Praweda Ciptakarsa Informatika) (Bachelor's thesis, Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta).

Mufti, R. G., Suprapto, S., & Mursityo, Y. T. (2017). Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 1(12), 1622-1631.

Nugroho, R., Suryono, R. R., & Darwis, D. (2016). Audit Tata Kelola Teknologi Informasi Untuk Integritas Data Menggunakan Framework Cobit 5 Pada Pt Kereta Api Indonesia (Persero) Divre Iv Tnk. Jurnal Teknoinfo, 10(1), 20-25.

P. N. Anastasia and L. H. Atrinawati, "Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 Pada Hotel XYZ," JSI: Jurnal Sistem Informasi (E-Journal), vol. 12, no. 2, Art. no. 2, Oct. 2020, doi: 10.36706/jsi.v12i2.12329.

R. Fauzan and R. Latifah, "Audit Tata Kelola Teknologi Informasi Untuk Mengontrol Manajemen Kualitas Menggunakan Cobit 4.1 (Studi Kasus : PT Nikkatsu Electric Works)," Jurnal Teknik Informatika Dan Sistem Informasi, 2015, doi: 10.28932/jutisi.v1i3.402.

R. Lombardi, M. D. Giudice, A. Caputo, F. Evangelista, and G. L. Russo, "Governance and Assessment Insights in Information Technology: The Val IT Model," Journal of the Knowledge Economy, 2015, doi: 10.1007/s13132-015-0328-6.

S. Turedi and H. Zhu, "How to Generate More Value From IT: The Interplay of IT Investment, Decision Making Structure, and Senior Management Involvement in IT Governance," Communications of the Association for Information Systems, 2019, doi: 10.17705/1cais.04426.

Shamgita, I. G. Y., Raditya, I. G. L. A., & Putra, I. G. J. E. (2020). Analisis Dan Evaluasi Tata Kelola Teknologi Informasi USSI Software Menggunakan Framework COBIT 5 Pada PT. BPR Naga. Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, 9(1), 67-74.

Sofa, K., Suryanto, T. L. M., & Suryono, R. R. (2020). Audit Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 Pada Dinas Pekerjaan Umum Kabupaten Tanggamus. Jurnal Teknologi Dan Sistem Informasi, 1(1), 39-46.

Suryono, R. R., Darwis, D., & Gunawan, S. I. (2018). Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 (Studi Kasus: Balai Besar Perikanan Budidaya Laut Lampung). Jurnal Teknoinfo, 12(1), 16-22.

Wicaksono, M. A., Rahardja, Y., & Chernovita, H. P. (2020). Analisis Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Domain Edm. JSiI (Jurnal Sist. Informasi), 7(1), 25.