PENTINGNYA SISTEM INFORMASI AUDIT DALAM MENINGKATKAN KEAMANAN DATA PERUSAHAAN

Nur Indah Septiyani Sirait[1] Muhammad Irwan Padli Nasution[2]
Fakultas Ekonomi Dan Bisnis Islam,Universitas Islam Negeri Sumatera Utara
Jl.William Iskandar,Ps.V Medan Estate,20371,Medan,Indonesia
Email: nurindahseptiyani0,gmail.com[1] irwannst@uinsu.ac.id[2]

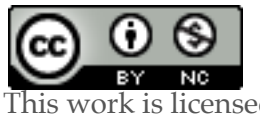
Abstrak:
Adapun tujuan utama dari research paper ini yaitu untuk menganalisis bagaimana Keamanan data perusahaan menjadi aspek penting yang harus diperhatikan di era digital saat ini.Ketika ancaman dunia maya menjadi lebih kompleks dan canggih, bisnis memerlukan sistem yang dapat memantau dan memastikan keamanan data secara keseluruhan.Cara efektif untuk mencapai hal ini adalah dengan menerapkan Sistem Informasi Audit (SIA).SIA memungkinkan bisnis untuk memantau aktivitas dalam sistem informasi mereka, mendeteksi potensi ancaman, dan mengidentifikasi kerentanan keamanan dengan cepat dan akurat.Melalui mekanisme verifikasi otomatis terstruktur, bisnis dapat menjaga integritas, ketersediaan, dan kerahasiaan data. Penelitian ini menjelaskan konsep dasar sistem keamanan database , jenis sistem keamanan database, dan teknologi terkini yang tersedia untuk meningkatkan keamanan database.Diuraikan juga bahaya yang dapat timbul jika sistem keamanan database tidak dijaga dengan baik, dan strategi untuk mengatasi masalah keamanan database.Penelitian ini bertujuan untuk lebih memahami pentingnya menjaga keamanan database bagi organisasi dan Perusahaan.Penulisan paper ini menggunakan metode deskriptif-kualitatif serta juga menggunakan Teknik study literatur yang dimana penulis ini meninjau beberapa hasil penelitian dari penelitian atau paper sebelumnya yang telah di publish,sehingga dapat menghasilkan sebuah kerangka teori baru yang didapat dari hasil mereview beberapa artikel/jurnal yang berhubungan dengan paper ini.Hasil penelitian ini juga didapat bahwa penerapan SIA tidak hanya memperkuat sistem keamanan data, namun juga meningkatkan kepatuhan terhadap peraturan dan standar keamanan yang berlaku.Selain itu, SIA juga dapat meminimalkan risiko penyalahgunaan data oleh pihak internal dan eksternal.Kesimpulan penelitian menunjukkan bahwa penerapan SIA yang efektif merupakan investasi strategis bagi bisnis untuk meningkatkan perlindungan data, melindungi reputasi mereka, dan meningkatkan kepercayaan pelanggan terhadap keamanan data mereka.

Kata Kunci:Sistem Informasi Audit,K eamanan Data,Perusahaan,Risiko Siber,Kepatuhan.

Abstract:
The main objective of this research paper is to analyze how company data security has become an important aspect that must be considered in the current digital era. As cyber threats become more complex and sophisticated, businesses need a system that

Article History
Received: November 2024
Reviewed: November 2024
Published: November 2024

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



This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

can monitor and ensure overall data security. How to effective way to achieve this is by implementing an Audit Information System (SIA).SIA allows businesses to monitor activities in their information systems, detect potential threats, and identify security vulnerabilities quickly and accurately.Through a structured automatic verification mechanism, businesses can maintain integrity, availability and confidentiality of data. This research explains the basic concepts of database security systems, types of database security systems, and the latest technology available to improve database security.It also describes the dangers that can arise if the database security system is not maintained properly, and strategies for overcoming database security problems.This research aims to better understand the importance of maintaining database security for organizations and businesses.The writing of this paper uses a descriptive-qualitative method and also uses a literature study technique in which the author reviews several research results from previous research or papers that have been published, so as to produce a new theoretical framework obtained from the results of reviewing several articles/journals related to this paper. The results of this research also show that the implementation of SIA not only strengthens the data security system, but also increases compliance with applicable regulations and security standards. Apart from that, SIA can also minimize the risk of data misuse by internal parties and external.The research conclusions show that effective implementation of SIA is a strategic investment for businesses to improve data protection, protect their reputation, and increase customer confidence in the security of their data.

Keywords: Audit Information System, Data Security, Company, Cyber Risk, Compliance.

A.PENDAHULUAN DAN LATAR BELAKANG

Di era digital saat ini, penggunaan database menjadi hal yang sangat penting dan lazim di berbagai bidang seperti bisnis, pendidikan, dan pemerintahan.Dalam penggunaannya, database menyimpan berbagai informasi sensitif seperti data keuangan, data pribadi, data akademik, dll.Oleh karena itu, keamanan database sangat penting untuk melindungi informasi sensitif yang disimpan di sana.Dalam konteks ini, peningkatan keamanan database telah menjadi prioritas utama, seiring dengan semakin sulitnya keamanan database seiring dengan semakin kompleksnya teknologi dan jumlah data yang disimpan.Selain itu, keamanan sistem database juga menjadi semakin rentan akibat serangan siber yang semakin canggih .Oleh karena itu, penelitian terhadap sistem keamanan database sangat relevan dan penting.

Ilmu pengetahuan dan teknologi informasi kini memainkan peran penting dalam organisasi, dan teknologi diperlukan untuk meningkatkan daya saing bisnis dan organisasi di hampir setiap sektor perekonomian.Kehadiran TI berperan penting dalam meningkatkan praktik tata kelola organisasi sebagai proses bisnis penting biasanya bersifat otomatis dan berdasarkan informasi yang disediakan oleh sistem TI sebagai pengambil keputusan.Ketergantungan terhadap TI ini mengharuskan organisasi memberikan perhatian khusus pada tata kelola.Tata kelola terdiri dari kepemimpinan, struktur organisasi, dan proses bisnis yang memastikan bahwa TI yang diadopsi oleh suatu organisasi berkembang dan selaras dengan strategi dan tujuannya.

Namun, TI yang digunakan mungkin tidak beroperasi secara optimal pada saat implementasi sehingga mengganggu proses bisnis yang sedang berjalan.Akibatnya, beberapa atau seluruh kegiatan yang telah disepakati dapat digagalkan, sehingga menyebabkan kegagalan atau kerusakan.Oleh karena itu, sistem informasi perlu diaudit agar temuan yang diperoleh selama audit dapat diterjemahkan menjadi rekomendasi atau saran untuk pengembangan TI dalam organisasi.Tujuan utama audit adalah mengumpulkan bukti obyektif, menganalisis bukti tersebut, dan membandingkannya dengan persyaratan yang ditentukan.Dengan melakukan audit sistem informasi, suatu organisasi dapat mempelajari seberapa baik proses bisnisnya, teknologi informasi yang digunakan, dan strategi bisnisnya selaras.

Audit adalah kegiatan pengumpulan dan pengujian data yang dilakukan oleh pihak yang kompeten dan independen untuk menentukan apakah informasi yang dikaji konsisten dengan standar yang telah ditetapkan dan dapat disajikan kepada pemangku kepentingan.Audit sistem informasi memungkinkan auditor mengumpulkan data dan bukti untuk memastikan bahwa sistem komputer yang sudah beroperasi dapat menjalankan fungsinya secara optimal untuk mencapai tujuan organisasi secara efektif dan menggunakan sumber daya secara efisien Sedangkan menurut Gondodiyot , audit sistem informasi adalah tingkat kepatuhan antara aplikasi dan sistem informasi yang diterapkan, dirancang, dan diterapkan oleh perusahaan sedemikian rupa sehingga memungkinkan perusahaan beroperasi secara optimal untuk mencapai tujuan bisnisnya.Ini didefinisikan sebagai survei yang dilakukan untuk mengukur.Saat mengaudit sistem informasi, target auditnya adalah departemen TI.

Di era digital saat ini, data perusahaan merupakan aset yang sangat berharga.Keamanan data adalah prioritas utama bagi setiap bisnis, terutama mengingat meningkatnya ancaman siber. Cara efektif untuk memastikan keamanan data adalah melalui audit kepatuhan keamanan informasi.Artikel ini menjelaskan peran audit kepatuhan keamanan informasi dalam melindungi data perusahaan dan bagaimana standar ISO 27001 dapat membantu.

Dengan pesatnya perkembangan teknologi dan meningkatnya ancaman dunia maya, sistem informasi telah menjadi tulang punggung sebagian besar bisnis.Tanpa audit, risiko pelanggaran data, serangan siber, dan ketidakpatuhan akan sangat tinggi.Sebagai bisnis yang memanfaatkan teknologi informasi, Anda perlu memahami bahwa sistem yang kuat dan tertata akan memperkuat posisi bisnis Anda di pasar.

Pentingnya audit sistem informasi pada suatu perusahaan adalah untuk memastikan bahwa seluruh elemen teknis mulai dari perangkat lunak dan perangkat keras hingga prosedur pengelolaan data berfungsi dengan baik.Ini akan membantu Anda menghindari kerugian besar yang mungkin terjadi akibat kerusakan sistem dan perlindungan informasi.

Di era digital saat ini, keamanan data menjadi prioritas utama bagi bisnis dan organisasi. Ketika ancaman dunia maya menjadi lebih kompleks, perlindungan data tidak bisa dianggap enteng.Alasan penting mengapa proses ini sangat diperlukan adalah:

1. Meningkatkan keamanan sistem dan data: Audit membantu mengidentifikasi kerentanan dalam sistem keamanan. Hal ini berlaku baik dari sudut pandang teknis maupun politik dan dapat dieksploitasi oleh penjahat dunia maya.
2. Kepatuhan: Banyak negara dan industri memiliki peraturan perlindungan data khusus, seperti GDPR Uni Eropa atau undang-undang PDP di Indonesia.
3. Audit memastikan bahwa perusahaan mematuhi peraturan ini dan menghindari denda yang mahal karena ketidakpatuhan.
4. Penyebab pelanggaran data: Audit rutin dapat membantu bisnis mencegah pelanggaran data sebelum terjadi.
5. Hal ini mengurangi risiko kerusakan dan kerugian finansial akibat insiden keamanan.
6. Meningkatkan prosedur internal: Audit juga mengungkapkan prosedur internal perusahaan mengenai pemrosesan data dan memastikan bahwa karyawan memahami dan mematuhi kebijakan keamanan yang ada.

B.METODE RISET

Dalam penyusunan paper ini, penulis menggunakan jenis metode penelitian deskriptif kualitatif dengan menggunakan wawancara berdasarkan focus group Discussion (FGD), yang mengacu pada teori dan penjelasan umum dari berbagai sumber. Beberapa data penelitian masa lalu.Kemudian dijelaskan dan dirinci untuk mendapatkan data yang berkualitas tinggi.Dalam jurnal ini, penulis juga menggunakan teknik tinjauan pustaka untuk memandu penyusunan makalah/jurnal akademik ini.Metode tinjauan pustaka bertujuan untuk mengumpulkan seluruh data/contoh berupa hasil tinjauan pustaka yang berkaitan dengan teori review hasil penelitian masa lalu.

Sebagai langkah awal dalam penulisan dan penyuntingan jurnal ini, penulis membuat studi kasus dan mengaitkannya dengan suatu isu atau informasi yang berkaitan dengan tema jurnal ini yaitu "Pentingnya Sistem Informasi Audit dalam Meningkatkan Keamanan Data Perusahaan".Setelah memilih beberapa topik terkait judul yang akan dibahas, langkah selanjutnya penulis menggunakan teknik persiapan tinjauan pustaka untuk melakukan analisis, tinjauan, dan pengolahan berdasarkan tinjauan pustaka tersebut.Penulis mengambil sampel/menganalisis sumber data berdasarkan Google Cendekiawan - Melalui ekstraksi basis data dan pemrosesan artikel/jurnal dari berbagai platform penerbitan dan berdasarkan permintaan pencarian yang dipublikasikan atau tidak, dan berbagai situs web resmi lainnya, bagaimana perbandingannya dengan penelitian sebelumnya.Penelitian teoretis baru dapat dilakukan dengan menganalisis, menjelaskan, dan mengisi kesenjangan dan kekurangan jika ada.Kerangka ini diharapkan dapat dibangun dari hasil penelitian para peneliti sebelumnya.Isi buku ini juga membandingkan teori dan hasil penelitian para peneliti sebelumnya dengan teori dan hasil penelitian terbaru yang dirangkum penulis.

C.HASIL DAN PEMBAHASAN

1..Pentingnya Audit Sistem Informasi

Audit sistem informasi adalah aktivitas yang berguna untuk dilakukan perusahaan secara rutin.Audit sistem informasi yang dilakukan pada suatu perusahaan bertujuan untuk mengukur kinerja sistem yang ada di perusahaan untuk mengetahui apakah kinerjanya sudah optimal dan dapat memberikan rekomendasi untuk mengoptimalkan sistem perusahaan tersebut.Investasi TI yang mahal diimbangi dengan keuntungan yang diterima perusahaan dari layanan dan operasi.Tentu saja, itu juga harus aman, andal, dan tidak mudah rusak.Audit sistem informasi memberikan keyakinan kepada organisasi bahwa TI yang sedang berlangsung dilindungi, memberikan informasi yang dapat diandalkan kepada pengguna, dan dikelola dengan baik untuk mencapai tujuan TI.Audit sistem informasi juga membantu mengurangi risiko manipulasi data, kehilangan atau kebocoran data, gangguan layanan, dan kesalahan manajemen sistem TI.Audit sistem informasi juga membantu perusahaan mempertahankan keunggulan kompetitifnya dan mencapai keuntungan yang dicapai perusahaan dalam jangka waktu tertentu.

Audit keamanan informasi adalah proses evaluasi yang bertujuan untuk memastikan bahwa sistem keamanan informasi suatu perusahaan mematuhi standar dan peraturan yang berlaku.Audit ini mencakup peninjauan terhadap kebijakan, prosedur, dan kontrol teknis yang diterapkan untuk melindungi data Anda dari ancaman internal dan eksternal.

Keamanan basis data merupakan proses yang sangat penting untuk memastikan bahwa data yang disimpan dalam basis data terlindungi dan tetap tersedia.Proses keamanan ini mencakup banyak langkah untuk memastikan bahwa hanya pihak yang berwenang yang memiliki akses terhadap data dan pihak yang tidak berwenang tidak dapat mengakses data tersebut. Keamanan basis data mencakup berbagai aspek seperti kebijakan keamanan, manajemen akses, enkripsi data, pencadangan dan pemulihan , pemantauan dan pemantauan. Kebijakan keamanan basis data adalah seperangkat pedoman dan aturan untuk memastikan bahwa data Anda tetap terlindungi dan tidak dapat disalahgunakan.Manajemen akses, di sisi lain, adalah tentang mengatur hak akses pengguna dalam database sehingga hanya pengguna yang berwenang yang dapat mengakses data yang disimpan.

Audit sistem informasi pada dasarnya adalah pemeriksaan komprehensif terhadap infrastruktur TI dalam suatu perusahaan.Pastikan sistem Anda yang ada berfungsi sesuai

harapan, memenuhi standar keselamatan, dan mematuhi peraturan yang ada.Kesenjangan dan kerentanan dalam sistem Anda dapat menjadikan perusahaan Anda sasaran empuk bagi peretas dan melindungi data Anda.

Pentingnya audit keamanan informasi dalam melindungi data perusahaan. Berikut adalah beberapa alasan mengapa audit ini penting:

- Identifikasi Kelemahan Keamanan:Audit membantu menemukan kelemahan dalam sistem keamanan yang mungkin tidak disadari oleh perusahaan. Dengan mengetahui kelemahan ini, perusahaan bisa melakukan perbaikan yang diperlukan.
- Meningkatkan Kepercayaan Pemangku Kepentingan:Jika perusahaan bisa menunjukkan kepatuhan pada standar keamanan informasi, seperti ISO 27001, maka akan meningkatkan kepercayaan dari klien, mitra bisnis, dan pemangku kepentingan lainnya.
- Pencegahan Insiden Keamanan:Audit reguler membantu mencegah insiden keamanan dengan memastikan bahwa semua langkah pencegahan dan respons terhadap ancaman sudah dilaksanakan dan berjalan dengan baik.

Bayangkan menjalankan perusahaan besar yang menangani berbagai data penting, termasuk informasi pelanggan, laporan keuangan, strategi bisnis, dan banyak lagi.Kegagalan dalam memelihara sistem informasi tidak hanya dapat mengakibatkan kerugian yang cukup besar, namun juga mengakibatkan menurunnya kepercayaan pelanggan dan mitra bisnis. Selain itu, pentingnya audit sistem informasi pada perusahaan juga terkait dengan kepatuhan terhadap berbagai regulasi yang terus berkembang, seperti General Data Protection Regulation (GDPR) Eropa dan regulasi perlindungan data di Indonesia.Tanpa audit yang tepat, perusahaan dapat menghadapi masalah hukum jika mereka gagal mengikuti aturan-aturan ini.

ISO 27001 adalah standar internasional untuk Sistem Manajemen Keamanan Informasi (ISMS). Standar ini memberikan kerangka kerja untuk mengelola keamanan informasi. Standar ini memberikan petunjuk kepada perusahaan dalam mengelola dan melindungi data secara teratur. Beberapa manfaat dari menggunakan ISO 27001 dalam audit keamanan informasi meliputi:

1. Pendekatan Sistematis
2. Peningkatan Kontrol Keamanan
3. Pemantauan dan Penilaian Terus-Menerus

2.Tujuan Keamanan Data

Tujuan dari keamanan basis data adalah untuk melindungi informasi yang disimpan dalam basis data dari akses yang tidak sah atau tidak diinginkan dan untuk memastikan bahwa data tetap rahasia, utuh, dan hanya dapat diakses oleh pihak yang berwenang.Tujuan utama keamanan basis data adalah:

1. Kerahasiaan:Basis data adalah untuk memastikan bahwa informasi yang disimpan dalam basis data bersifat rahasia dan tidak dapat diakses oleh orang yang tidak berwenang.Hal ini dapat dicapai dengan menerapkan sistem otentikasi yang kuat dan menetapkan hak akses dan enkripsi data yang sesuai.
2. Integritas:Database adalah untuk memastikan bahwa data dalam database tetap utuh dan tidak dapat dirusak atau dimanipulasi oleh pihak yang tidak berkepentingan.Hal ini dapat dicapai dengan menggunakan teknologi checksum atau tanda tangan digital dan menerapkan sistem validasi data yang ketat.
3. Ketersediaan:Basis data adalah untuk memastikan bahwa data tetap tersedia bagi pihak yang berwenang dan tidak dapat dikompromikan oleh serangan atau intrusi sistem.Hal ini dapat dicapai melalui penggunaan sistem pencadangan dan pemulihan yang efektif, teknologi penyeimbangan beban, dan pemantauan sistem yang berkelanjutan oleh .
4. Kepatuhan:Database adalah untuk memastikan kepatuhan terhadap peraturan dan aturan perlindungan data yang berlaku seperti GDPR, HIPAA, dll.Hal ini dapat dicapai dengan menerapkan kebijakan keamanan yang tepat dan melakukan audit secara berkala untuk memastikan bahwa sistem keamanan database tetap sesuai dengan persyaratan yang berlaku.

Secara keseluruhan, tujuan keamanan basis data adalah untuk melindungi informasi sensitif dan penting dari korupsi, pencurian, dan penggunaan tidak sah, dan untuk memastikan bahwa data hanya tersedia untuk pihak yang berwenang.Dengan menerapkan sistem keamanan yang tepat, bisnis dapat menjaga data mereka tetap aman dan terlindungi dari ancaman keamanan yang muncul.

4.Manfaat Audit Untuk Perusahaan

1. Peningkatan kepercayaan pelanggan: pelanggan mengalami peningkatan kepercayaan terhadap perusahaan yang menjaga keamanan data mereka.Dengan melakukan audit rutin, perusahaan dapat menunjukkan komitmennya dalam melindungi data pelanggan.
2. Mengurangi risiko finansial: Pelanggaran data dapat menyebabkan kerugian finansial yang signifikan.Audit keamanan memungkinkan organisasi untuk mengidentifikasi dan mengatasi potensi risiko sebelum insiden terjadi, sehingga meminimalkan kerugian.
3. Meningkatkan efisiensi operasional: Audit juga membantu perusahaan menemukan kerentanan dalam sistem dan proses bisnis yang dapat berdampak pada efisiensi.Mengatasi masalah ini akan membantu bisnis beroperasi lebih efisien dan aman.
4. Kepatuhan terhadap Peraturan: Kepatuhan privasi sangat penting bagi bisnis, terutama di sektor yang memiliki regulasi ketat seperti perbankan, layanan kesehatan, dan teknologi.Audit memastikan bahwa perusahaan mematuhi semua persyaratan hukum dan membantu menghindari denda yang mahal.

-Mengurangi Risiko Serangan Siber

Salah satu ancaman terbesar terhadap bisnis saat ini adalah serangan siber.Di era digital, hacker semakin canggih dan metode serangannya semakin sulit diprediksi.Pemeriksaan informasi sistem membantu memastikan bahwa sistem keamanan Anda memenuhi standar industri dan dapat menahan serangan eksternal.Audit membantu mengidentifikasi potensi kesenjangan dalam sistem keamanan Anda.Penting untuk menjawab pertanyaan-pertanyaan ini melalui audit.

-Meningkatkan Efisiensi Bisnis Audit sistem informasi

Tidak hanya dari sudut pandang keamanan, tetapi juga untuk meningkatkan efisiensi bisnis perusahaan.Dengan mengidentifikasi dan menghapus komponen yang tidak efisien atau usang, bisnis dapat meningkatkan kinerja sistem secara keseluruhan. Misalnya, perangkat lunak yang ketinggalan jaman atau perangkat keras yang lambat dapat memengaruhi produktivitas.Audit tersebut memberikan rekomendasi untuk mengganti atau memperbarui teknologi yang digunakan.Mengingat pentingnya audit sistem informasi dalam organisasi, penting untuk tidak hanya memperkuat keamanan tetapi juga memastikan bahwa seluruh bagian sistem beroperasi pada kapasitas optimal.Hal ini tentunya akan berdampak positif terhadap operasional perusahaan sehari-hari.Audit ini adalah kunci untuk menjaga keamanan, efisiensi, dan kepatuhan terhadap peraturan di era digital yang penuh tantangan.Melakukan audit secara rutin dapat melindungi bisnis Anda dari ancaman dunia maya, mengoptimalkan penggunaan teknologi, dan menjaga integritas data.

4.Jenis-Jenis Audit Dalam Sistem

Berbagai jenis audit keamanan data dapat dilakukan, bergantung pada kebutuhan perusahaan dan tujuan audit.

1. Audit Kepatuhan: Audit ini berfokus pada penilaian apakah suatu perusahaan mematuhi peraturan dan standar perlindungan data yang berlaku. Contoh: GDPR, HIPAA,ISO 27001.Tujuannya adalah untuk memastikan bahwa semua kebijakan dan prosedur keamanan mematuhi peraturan yang ditetapkan.
2. Audit Risiko: Audit ini mengevaluasi potensi risiko yang mungkin dihadapi perusahaan terkait keamanan data.Auditor menilai infrastruktur teknologi dan proses bisnis untuk mengidentifikasi kerentanan yang dapat dieksploitasi oleh penjahat dunia maya.
3. Ujian Sistem Teknologi Informasi (TI): Ujian ini berfokus pada infrastruktur teknologi yang digunakan dalam organisasi, termasuk perangkat keras, perangkat lunak, jaringan, dan sistem keamanan.Tujuannya untuk memastikan seluruh komponen teknologi berfungsi dengan baik dan terlindungi dari serangan.

5.Langkah-Langkah Dalam Melakukan Audit Kepatuhan Keamanan Informas

Langkah-langkah umum yang biasanya dilakukan selama audit kepatuhan keamanan informasi adalah:

1. Perencanaan Audit: Menentukan tujuan, ruang lingkup, dan jadwal audit.
2. Pengumpulan Data: Mengumpulkan informasi melalui wawancara, survei, dan dokumentasi terkait kebijakan dan prosedur keamanan informasi.
3. Penilaian dan Analisis: Menganalisis data yang dikumpulkan untuk mengidentifikasi risiko keamanan.
4. Laporan Temuan:Membuat laporan audit yang mencakup temuan, rekomendasi perbaikan, dan rencana tindakan.
5. Tindak lanjut: mengartikan bahwa seluruh rekomendasi perbaikan telah dilaksanakan dan diuji keefektifannya.

D.PENUTUP

Oleh karena itu, gagasan teoritis para penulis dalam jurnal ini sebenarnya memerlukan penelitian lebih lanjut yang relevan mengenai topik dan pembahasan tersebut, serta hasil teoritis baru yang diperoleh dari penelitian-penelitian sebelumnya.Hal ini bertujuan untuk menjaga relevansi teori dan temuan penelitian dengan perubahan kondisi di masa depan. Penulis berharap jurnal ini dapat menjadi referensi khususnya dalam bidang Sistem informasi audit berperan penting dalam meningkatkan keamanan data perusahaan dengan mendeteksi, mencegah, dan mengatasi ancaman terhadap data.Sistem ini memungkinkan perusahaan untuk menjaga aktivitas bisnis dan mendokumentasikan seluruh proses terkait data manajemen secara detail.Melalui audit terstruktur dan otomatis, bisnis dapat mengidentifikasi kerentanan dan mengambil tindakan pencegahan untuk mencegah risiko keamanan seperti kebocoran data, akses tidak sah, dan transmisi informasi sensitif.Sistem informasi audit juga berfungsi sebagai alat untuk memverifikasi kepatuhan perusahaan terhadap peraturan perlindungan data yang berlaku, sehingga meminimalkan risiko denda dan pelanggaran hukum.Kesimpulannya, penerapan sistem informasi audit merupakan langkah strategis untuk memperkuat keamanan data perusahaan, menjaga integritas informasi, dan meningkatkan kepercayaan pihak-pihak terkait terhadap keamanan data yang dikelola perusahaan.

E.REFERENSI

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. https://doi.org/10.47233/jiska.v1i2.929

Oktania Purwaningrum, Baitun Nadhiroh2,Siti Mukaromah (2021). Literatur Riview Audit Sistem Informasi Menggunakan Kerangka Kerja Cobit 5.*Jurnal Informatika dan Sistem Informasi (JIFoSI)*

https://integrasolusi.com/blog/peran-audit-kepatuhan-keamanan-informasi-dalam-melindungi-data-perusahaan/

https://widyasecurity.com/2024/09/10/audit-keamanan-data-pengertian-jenis-dan-pentingnya/

https://blog.unmaha.ac.id/pentingnya-audit-sistem-informasi-dalam-perusahaan/

Clara Valentine Febiolla, Dorkas Setiawaty (2020) Audit Sistem Informasi Berbasis Iso 27001Diera New Normal *Prosiding ASIC 2020*