e-ISSN:2829-4580, p-ISSN: 2829-4599
DOI: https://doi.org/10.38035/jim.v2i1
Received: 17 Mei 2023, Revised: 12 Juni 2023, Publish: 13 Juni 2023

JIM
JURNAL ILMU MULTIDISIPLIN
E-ISSN:2829-4580, P-ISSN=2829-4599
https://greenpub.org/JIM
editor@greenpub.org
0811 7401 455

Peran CIA (*Confidentiality, Integrity, Availability*) Terhadap Manajemen Keamanan Informasi

Rayhan Vansuri[1], Achmad Fauzi[2], Ery Teguh Prasetyo[3], Riga Negara[4], Rifqi Ramadhan[5], Alfian Mada Restu[6], Raditya Raffi Firmansyah[7]
[1.] Universitas Bhayangkara Jakarta Raya, Indonesia, 202010325360@mhs.ubharajaya.ac.id
[2.] Universitas Bhayangkara Jakarta Raya, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3.] Universitas Bhayangkara Jakarta Raya, Indonesia, ery.teguh@ubharajaya.ac.id
[4.] Universitas Bhayangkara Jakarta Raya, Indonesia, 202010325416@mhs.ubharajaya.ac.id
[5.] Universitas Bhayangkara Jakarta Raya, Indonesia, 202010325331@mhs.ubharajaya.ac.id
[6.] Universitas Bhayangkara Jakarta Raya, Indonesia, 202010325359@mhs.ubharajaya.ac.id
[7.] Universitas Bhayangkara Jakarta Raya, Indonesia, 202010325344@mhs.ubharajaya.ac.id

Corresponding Author: Rayhan Vansuri

Abstract: *In this case, information security is an important factor that must be considered by every company. However, information security is often ignored or not taken seriously by companies. Some of the factors that cause this are the lack of awareness and knowledge about information security and the lack of training for employees in managing information and technology. This research uses a literature study method. In addition, this study also discusses the role of training and security awareness in information security management in companies. The results of the study explain that security training and awareness play an important role in information security management in companies. Good security training and awareness can help employees and managers to be more aware of information security threats, and help companies to ensure better information security and protect the interests of companies and customers.*

Keyword: *Information Security, Awareness, Training, Company.*

Abstrak: Dalam hal ini, keamanan informasi merupakan faktor penting yang harus diperhatikan oleh setiap perusahaan. Namun, keamanan informasi seringkali diabaikan atau tidak dianggap serius oleh perusahaan. Beberapa faktor yang menyebabkan hal tersebut adalah kurangnya kesadaran dan pengetahuan tentang keamanan informasi serta kurangnya pelatihan bagi karyawan dalam mengelola informasi dan teknologi. Penelitian ini menggunakan metode studi literatur. Selain itu, penelitian ini juga membahas peran pelatihan dan kesadaran keamanan dalam manajemen keamanan informasi di perusahaan. Hasil penelitian menjelaskan bahwa pelatihan dan kesadaran keamanan berperan penting dalam manajemen keamanan informasi di perusahaan. Pelatihan dan kesadaran keamanan yang baik

dapat membantu karyawan dan manajer untuk lebih waspada terhadap ancaman keamanan informasi, dan membantu perusahaan memastikan keamanan informasi yang lebih baik dan melindungi kepentingan perusahaan dan pelanggan.

Kata Kunci: Keamanan Informasi, Kesadaran, Pelatihan, Perusahaan.

PENDAHULUAN

Karena semakin banyak bisnis yang bergantung pada teknologi dan informasi untuk menjalankan operasinya, keamanan informasi menjadi perhatian yang lebih penting di lingkungan perusahaan saat ini. Data dan informasi yang dikumpulkan, diproses, dan disimpan oleh bisnis menjadi aset strategis yang penting. Keamanan informasi merupakan pertimbangan penting bagi setiap perusahaan dalam situasi ini. Namun, seringkali keamanan informasi diabaikan atau tidak diperhatikan secara serius oleh perusahaan. Beberapa faktor yang menjadi penyebab hal ini adalah kurangnya kesadaran dan pengetahuan mengenai keamanan informasi serta kurangnya pelatihan bagi karyawan dalam mengelola informasi dan teknologi.

Penelitian sebelumnya menunjukkan bahwa pelatihan dan kesadaran keamanan informasi sangat penting untuk memastikan keamanan informasi di perusahaan. Tanpa pelatihan dan kesadaran keamanan informasi yang memadai, perusahaan dapat menjadi rentan terhadap serangan siber dan kebocoran data.

Pelatihan keamanan informasi bertujuan untuk memberikan karyawan dengan pengetahuan dan keterampilan yang diperlukan untuk mengelola informasi dan teknologi dengan aman. Pelatihan ini dapat mencakup berbagai topik, seperti keamanan jaringan, enkripsi, tindakan keamanan di media sosial, dan kebijakan keamanan. Selain pelatihan, kesadaran keamanan informasi juga sangat penting. Pemahaman karyawan tentang bahaya keamanan informasi dan langkah-langkah yang harus diambil untuk mengurangi atau menghilangkannya dikenal sebagai kesadaran keamanan informasi. Memahami kata sandi aman, phishing, malware, dan prosedur keamanan mendasar lainnya adalah contoh kesadaran keamanan informasi.

Dalam jurnal ini, penulis membahas tentang pentingnya pelatihan dan kesadaran keamanan informasi dalam manajemen keamanan informasi di perusahaan. Mereka melakukan penelitian terhadap karyawan dari beberapa perusahaan untuk mengetahui seberapa baik perusahaan dalam memberikan pelatihan dan meningkatkan kesadaran keamanan informasi kepada karyawan mereka. Hasil penelitian menunjukkan bahwa sebagian besar karyawan tidak mendapatkan pelatihan keamanan informasi yang memadai dari perusahaan mereka. Selain itu, kesadaran keamanan informasi karyawan juga cenderung rendah. Hal ini dapat menjadi masalah serius karena karyawan yang tidak memiliki pengetahuan dan kesadaran yang cukup mengenai keamanan informasi dapat secara tidak sengaja atau disengaja memicu kebocoran data atau serangan siber.

Dalam studi ini, penulis juga menemukan bahwa perusahaan yang memberikan pelatihan dan meningkatkan kesadaran keamanan informasi cenderung memiliki keamanan informasi yang lebih baik. Mereka mampu mengurangi risiko kebocoran data dan serangan siber yang dapat membahayakan perusahaan dan pelanggan mereka. Dalam konteks manajemen keamanan informasi, risiko kebocoran data dan serangan siber dapat mengakibatkan kerugian finansial yang besar bagi perusahaan. Kerugian tersebut dapat berasal dari biaya pemulihan sistem, kehilangan kepercayaan pelanggan, hingga kerugian yang diakibatkan oleh pencurian data penting seperti data pelanggan, rahasia perusahaan, atau kekayaan intelektual.

Meningkatkan pelatihan dan kesadaran keamanan informasi di perusahaan dapat membantu mengurangi risiko tersebut dengan meningkatkan keterampilan dan pengetahuan karyawan dalam mengelola informasi dan teknologi dengan aman. Karyawan yang terampil dan sadar keamanan akan dapat mengenali ancaman keamanan informasi dan mengambil tindakan yang tepat untuk mencegah atau mengatasi ancaman tersebut. Selain itu, perusahaan yang memberikan pelatihan dan meningkatkan kesadaran keamanan informasi juga dapat meningkatkan kepatuhan terhadap kebijakan keamanan dan prosedur yang telah ditetapkan. Karyawan yang terlatih dan sadar keamanan akan lebih cenderung mematuhi kebijakan keamanan dan prosedur yang telah ditetapkan oleh perusahaan, sehingga mengurangi risiko kesalahan atau pelanggaran yang dapat mengancam keamanan informasi.

Dalam kesimpulannya, penelitian ini menunjukkan bahwa pelatihan dan kesadaran keamanan informasi merupakan faktor penting dalam manajemen keamanan informasi di perusahaan. Perusahaan yang memberikan pelatihan dan meningkatkan kesadaran keamanan informasi dapat mengurangi risiko kebocoran data dan serangan siber, serta meningkatkan kepatuhan terhadap kebijakan dan prosedur keamanan. Oleh karena itu, perusahaan harus memprioritaskan pelatihan dan kesadaran keamanan informasi bagi karyawan mereka untuk memastikan keamanan informasi yang lebih baik.

Rumusan Masalah

1. Apa Peran Confidentiality (Kerahasiaan) dalam Manajemen Keamanan Informasi di dalam Perusahaan?
2. Apa Peran Integrity (Integritas) dalam Manajemen Keamanan Informasi di Perusahaan?
3. Apa peran gabungan antara pelatihan keamanan dan kesadaran keamanan terhadap manajemen keamanan informasi di perusahaan?

Tujuan Penelitian

1. Menjelaskan bagaimana setiap elemen CIA dapat membantu organisasi dalam menjaga keamanan informasi dan aset penting mereka.
2. Untuk membantu persahaan dalam menjaga dan menerapkan confidentiality,integrity, availability dalam Manajemen keamanan informas
3. Memberikan panduan praktis bagi perusahaan dalam mengelola keamanan informasi mereka, termasuk pengembangan kebijakan keamanan informasi yang tepat, pelaksanaan tindakan pencegahan keamanan informasi yang efektif, dan pelatihan karyawan dalam praktik keamanan informasi yang baik.

METODE

Metode studi literatur digunakan dalam penelitian ini. Metode studi pustaka adalah suatu pendekatan penelitian yang melibatkan pengumpulan, mengevaluasi, dan menganalisis berbagai sumber informasi yang berhubungan dengan topik penelitian yang sedang diuji. Metode ini dilakukan dengan menggunakan bahan-bahan pustaka, seperti buku, jurnal, dan dokumen lainnya, sebagai data yang akan dianalisis. Metode studi pustaka sering digunakan untuk memperdalam pemahaman mengenai topik tertentu, melengkapi data yang sudah ada, atau membandingkan temuan penelitian yang sudah dilakukan sebelumnya. (Sukmadinata, 2014)

Tabel 1: Hasil Penelitian yang Relevan Terdahulu

No	Author (tahun)	Hasil Riset terdahulu	Persamaan dengan artikel ini	Perbedaan dengan artikel ini
1	Agus Purwanto, (2021)	Hasil Setelah pelatiha, peserta akan dapat memahami bagaimana	Kedua artikel membahas tentang peningkatan keamanan, dimana artikel	Artikel terdahulu membahas tentang keamanan pangan

		menerapkan persyaratan di tempat kerja masing-masing, mereka menerapkan Sistem Manajemen Keamanan Pangan ISO 22000:2018. Nilai evaluasi pretest tipikal adalah 24% sebelum pelatihan. Setelah pelatihan, skor rata-rata postes adalah 97%.	terdahulu membahas tentang keamanan pangan melalui pelatihan ISO 22000:2018 pada industri kemasan makanan, sedangkan artikel ini membahas tentang peran pelatihan dan kesadaran keamanan dalam manajemen keamanan informasi di perusahaan.	pada industri kemasan makanan, sedangkan jurnal ini membahas tentang keamanan informasi di perusahaan.
2	Rifqi Akmal Syarif, Agung Nugroho (2016)	Temuan penelitian menunjukkan bahwa keamanan informasi masih tergolong penerapan kerangka fundamental (Aktif) pada tingkat kematangan II untuk penerapan aplikasi SPAN. Teknologi informasi dan keamanan, dari enam bidang utama yang diperiksa, memperoleh skor terbesar (83%), namun manajemen risiko masih mendapat skor buruk dan perlu mendapat perhatian khusus dari Dirjen Perbendaharaan.	Kedua artikel membahas tentang keamanan informasi, dimana artikel sebelumnya membahas pemanfaatan Indeks keamanan Informasi untuk menganalisis sedangkan artikel ini membahas tentang fungsi pelatihan dan security awareness dalam manajemen keamanan informasi di dunia usaha, membahas tingkat kematangan sistem manajemen keamanan informasi Ditjen Perbendaharaan.	Artikel terdahulu membahas tentang analisis tingkat dengan Indeks keamanan Informasi, membahas pentingnya kesadaran keamanan dan pelatihan dalam manajemen keamanan informasi dalam bisnis sambil mengevaluasi keadaan sistem manajemen keamanan informasi Ditjen Perbendaharaan.
3	Dian Chisva Islami, Khodijah Bunga I.H, Candiwan (2016)	Temuan survei ini menunjukkan bahwa Bank X Bandung berhasil menerapkan aturan keamanan informasi, dan sebagian besar pekerja bank memiliki tingkat pengetahuan yang tinggi. tingkat keamanan data yang tinggi.	Kedua artikel tersebut membahas tentang kesadaran keamanan informasi.	Artikel terdahulu hanya membahas kesadaran staf keamanan informasi di Bank X di Bandung, Indonesia, sedangkan artikel ini membahas peran pelatihan dan kesadaran keamanan dalam manajemen keamanan informasi di perusahaan secara umum.
4	Darmawan Setiya Budi, Avinanta Tarigan (2018)	Strategi dan implementasi keamanan informasi yang lebih baik dapat dikembangkan di dalam organisasi dengan melakukan evaluasi menggunakan indeks kami untuk memastikan tingkat kesiapan dan kematangan perusahaan terhadap keamanan informasi. Indeks kami	Kedua artikel membahas tentang manajemen keamanan informasi, Artikel ini juga membahas tentang peran pelatihan dan kesadaran keamanan dalam manajemen keamanan informasi di perusahaan.	Artikel terdahulu membahas tentang prinsip dan metode pengukuran manajemen keamanan informasi dengan menggunakan Knowledge-Awareness-Maturity Index (KAMI) dan kesadaran pengguna terhadap keamanan informasi, sedangkan

		versi 3.1 berdasarkan ISO 27001:2013 adalah versi terbaru. Kesadaran keamanan informasi di kalangan pengguna dievaluasi menggunakan HAIS-Q berdasarkan komponen pengetahuan, sikap, dan perilaku (Model KAB). Karena orang menggunakan teknologi informasi dan merupakan mata rantai terlemah dalam keamanan informasi, evaluasi orang sangat penting. keamanan informasi.		artikel ini tidak membahas tentang evaluasi manajemen keamanan informasi secara spesifik dan lebih fokus pada peran pelatihan dan kesadaran keamanan dalam manajemen keamanan informasi di perusahaan.
5	Rokhman Fauzi (2018)	Hasil penelitian ini adalah dalam menggunakan pendekatan OCTAVE-S untuk analisis risiko, ditunjukkan bahwa perusahaan menghadapi tingkat risiko keamanan sedang dan menawarkan sejumlah metode mitigasi terkait kontrol ISO/IEC 27002.	Kedua artikel membahas tentang manajemen keamanan informasi.	Artikel terdahulu membahas tentang implementasi Sistem manajemen keamanan informasi berbasis kontrol ISO/IEC 27002 untuk UKM,, sedangkan artikel ini membahas tentang peran pelatihan dan kesadaran keamanan dalam manajemen keamanan informasi di perusahaan.

HASIL DAN PEMBAHASAN

CIA (Confidentiality, Integrity, Availability) sangat penting dalam manajemen keamanan informasi di perusahaan. Manajemen keamanan informasi yang efektif harus memastikan bahwa informasi dan aset penting dijaga dengan baik dan terlindungi dari ancaman keamanan (Pardini, Heinisch, & Parreiras, 2017).

Peran Confidentiality (Kerahasiaan) dalam Manajemen Keamanan Informasi di dalam Perusahaan

Penelitian ini bermaksud untuk menilai fungsi confidentiality dalam mengelola keamanan informasi dalam bisnis dan untuk membantu pembaca memahami betapa pentingnya kerahasiaan untuk menjaga data sensitif.

Hasil penelitian menunjukkan bahwa perusahaan yang memberikan confidentiality (Kerahasiaan) cenderung memiliki keamanan informasi yang lebih baik. Perusahaan-perusahaan tersebut menerapkan kebijakan keamanan informasi yang lebih ketat, menggunakan teknologi keamanan informasi yang lebih baik, dan lebih sering melakukan audit keamanan informasi daripada perusahaan yang tidak memberikan pelatihan keamanan. Selain itu, perusahaan-perusahaan yang memberikan confidentiality cenderung memiliki tingkat kepuasan pelanggan yang lebih tinggi. Hal ini menunjukkan bahwa pelatihan keamanan tidak hanya membantu melindungi informasi penting di perusahaan, tetapi juga memperkuat hubungan dengan pelanggan (Syarif, & Nugroho, 2016).

Dalam konteks ini, perusahaan harus mempertimbangkan pentingnya menerapkan confidentiality di perusahaan. confidentiality dapat membantu meningkatkan kerahasiaan keamanan tentang risiko keamanan informasi, serta membantu mereka untuk mengidentifikasi dan mengelola ancaman keamanan informasi dengan lebih efektif. Sebagai hasilnya, perusahaan dapat memastikan keamanan informasi yang lebih baik dan melindungi kepentingan perusahaan serta pelanggan.

Peran Integrity (Integritas) dalam Manajemen Keamanan Informasi di Perusahaan

Penelitian ini bermaksud untuk menilai nilai integritas dalam mengelola keamanan informasi dalam bisnis dan untuk menunjukkan betapa pentingnya meningkatkan kesadaran keamanan untuk melindungi data penting.Keutuhan adalah elemen kedua dalam manajemen keamanan informasi. Ini melibatkan perlindungan informasi dari perubahan atau modifikasi yang tidak sah (Khidzir et al., 2018). Dalam hal ini, organisasi harus memastikan bahwa informasi dan data tidak diubah atau dimanipulasi oleh pihak yang tidak berwenang. Hal ini dapat dicapai melalui penggunaan tanda tangan digital, log audit, dan tindakan pencegahan lainnya.

Hasil penelitian menunjukkan bahwa Integritas memainkan peran penting dalam melindungi informasi penting di perusahaan. Karyawan yang memiliki tingkat Integritas yang lebih tinggi cenderung lebih waspada terhadap ancaman keamanan informasi dan lebih mampu mengidentifikasi tindakan yang merugikan keamanan informasi. Selain itu, perusahaan-perusahaan yang mengutamakan kesadaran keamanan memiliki kebijakan keamanan informasi yang lebih baik dan lebih sering melakukan audit keamanan informasi daripada perusahaan yang tidak mengutamakan kesadaran keamanan(Kumar & Bhatia, 2020).

Peran Availability (Ketersediaan) dalam Manajemen Keamanan Informasi di Perusahaan

Tujuan dari penelitian ini adalah untuk menilai signifikansi ketersediaan dalam manajemen keamanan informasi perusahaan. Wawancara dengan manajer dan staf dari berbagai perusahaan Indonesia yang memiliki akses ke informasi penting dan sensitif digunakan untuk mengumpulkan data.

Perusahaan harus memastikan bahwa informasi dan sistem keamanan yang diperlukan dapat diakses ketika dibutuhkan. Hal ini dapat dicapai melalui penggunaan back-up dan pemulihan data, pengelolaan kapasitas dan ketersediaan sistem, dan tindakan pencegahan lainnya.

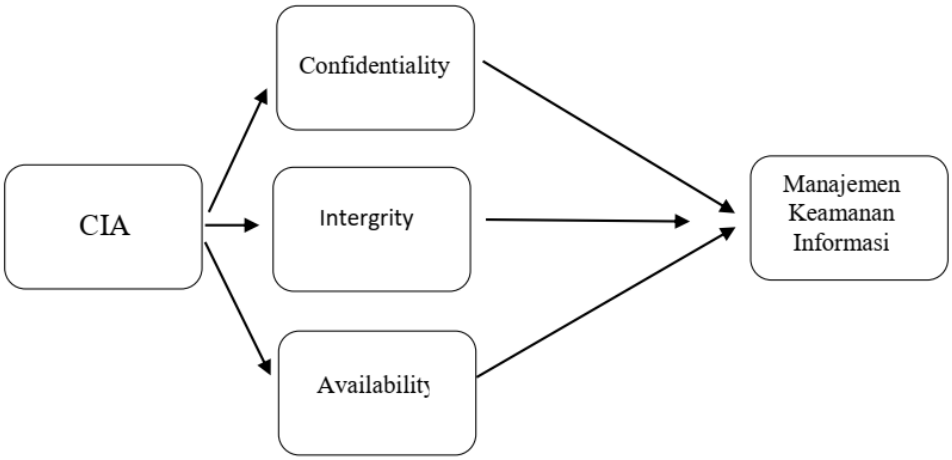
Hasil penelitian menunjukkan bahwa perusahaan yang menerapkan Availability (Ketersediaan) cenderung memiliki keamanan informasi yang lebih baik. Perusahaan-perusahaan tersebut menerapkan kebijakan keamanan informasi yang lebih ketat. Selain itu, perusahaan-perusahaan yang menerapkan availability cenderung memiliki kebijakan keamanan informasi yang lebih ketat dan lebih sering melakukan audit keamanan informasi (Avinanta Tarigan, 2018). Hal ini menunjukkan bahwa kesadaran keamanan informasi sangat penting dalam mencegah serangan siber dan kebocoran data.

Manajemen keamanan informasi yang efektif juga mencakup proses dan praktik yang menyeluruh untuk mengelola risiko keamanan informasi secara keseluruhan. Contohnya adalah pengembangan kebijakan keamanan informasi dan pelaksanaannya, pengelolaan identitas dan akses, pengelolaan keamanan jaringan dan sistem, dan pelatihan keamanan informasi bagi karyawan dan pemangku kepentingan lainnya (Fauzi 2018).

Dalam mengelola keamanan informasi di perusahaan, CIA dapat membantu perusahaan untuk mengidentifikasi dan mengelola risiko keamanan informasi dengan lebih efektif. Dengan menjaga kerahasiaan, keutuhan, dan ketersediaan informasi, perusahaan

dapat mengurangi risiko keamanan informasi dan melindungi aset penting mereka dari ancaman keamanan.

Conceptual Framework



Gambar 1: Conceptual Framework

Sesuai figure, maka dapat diketahui bahwa pelatihan dan kesadaran dalam Manajemen Kemanan Informasi di Perusahaan.

KESIMPULAN

Manajemen keamanan informasi yang efektif juga mencakup proses dan praktik yang menyeluruh untuk mengelola risiko keamanan informasi secara keseluruhan. Contohnya adalah pengembangan kebijakan keamanan informasi dan pelaksanaannya, pengelolaan identitas dan akses, pengelolaan keamanan jaringan dan sistem, dan pelatihan keamanan informasi bagi karyawan dan pemangku kepentingan lainnya.

Dalam mengelola keamanan informasi di perusahaan, CIA dapat membantu perusahaan untuk mengidentifikasi dan mengelola risiko keamanan informasi dengan lebih efektif. Dengan menjaga kerahasiaan, keutuhan, dan ketersediaan informasi, perusahaan dapat mengurangi risiko keamanan informasi dan melindungi aset penting mereka dari ancaman keamanan.

Saran bagi perusahaan harus mengembangkan strategi keamanan informasi yang komprehensif dan terintegrasi dengan mempertimbangkan aspek Confidentiality, Integrity, dan Availability (CIA). Perusahaan harus memastikan bahwa karyawan dan pemangku kepentingan lainnya memahami pentingnya keamanan informasi dan menerapkan praktik keamanan informasi yang tepat. Selain itu, perusahaan harus terus memantau dan mengevaluasi keamanan informasi mereka untuk mengidentifikasi dan mengatasi potensi risiko keamanan yang muncul.

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) dan Evaluasi Kesadaran Keamanan Informasi pada Pengguna. Jurnal Sistem Informasi Bisnis, 2(1).

Fauzi, R. (2018). Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002. Jurnal Sistem Informasi Bisnis, 3(2).

Islami, D. C., I.H, K. B., & Candiwan. (2016). Kesadaran Keamanan Informasi pada Pegawai Bank X di Bandung Indonesia. Jurnal Manajemen Teknologi, 10(1).

Siregar, N. S. (2016). Kesadaran masyarakat nelayan terhadap pendidikan anak. Jurnal Ilmu Pemerintahan dan Sosial Politik UMA, 4(1).

Sukmadinata, N. S. (2014). Metode Penelitian Pendidikan. Bandung: PT. Remaja Rosdakarya.

Syarif, R. A., & Nugroho, A. (2016). Analisis Tingkat Kematangan Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan Diukur dengan Menggunakan Indeks Keamanan Informasi (Studi Kasus: Aplikasi SPAN). Jurnal Ilmiah Ilmu Komputer, 4.

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.

B.E. Putro (2016) . Klausul A.5 Analisis Audit Penilaian Mandiri Pengendalian Kebijakan Keamanan Kebijakanpada Klausul A.9Analisis Audit Penilaian Sendiri Pengendalian pada Klausul A.9 27001, pengamanan fisik dan lingkungan Telkom Flexi Kebon Sirih Jakarta Pusat . 8(1)

Media Jurnal Informatika.Saefudin, A. N., Mulyani, Y., & Fathoni, A. (2021). Penerapan Metode Studi Pustaka dalam Penelitian Hukum Islam. Jurnal Hukum Islam, 5(1), 35-46.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022a). 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.

Pelayanan, M., Smk, P. Di, Mayasari, A., Supriani, Y., & Arifudin, O. (2021). Implementasi Sistem Informasi Manajemen Akademik Berbasis Teknologi Informasi dalam Meningkatkan. In *JIIP-Jurnal Ilmiah Ilmu Pendidikan* (Vol. 4, Issue 5). http://Jiip.stkipyapisdompu.ac.id

Puriwigati, A. N., & Buana, U. M. (2020). *Sistem Informasi Manajemen-Keamanan Informasi*. *May*. Riana, E., Eka, M., Sulistyawati, S., & Putra, O. P. (2023). *Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do- Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001 : 2013*. *4*(2), 632–640. https://doi.org/10.47065/josh.v4i2.2552