Nusantara Journal of Multidisciplinary Science
Vol. 2, No. 1, Januari 2024
Hal 94-102
E-ISSN : 3024-8752
P-ISSN : 3024-8744
Site : https://jurnal.intekom.id/index.php/njms

Peranan Penting Manajemen Sekuriti di Era Digitalisasi

Rio Fachrudin[1], Erlangga Respaty[2], Ipon Syawal Adilah[3], Fried Sinlae[4]
[1,2,3,4]Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Article Info

Article history:

Received Januari 01, 2024
Revised Januari 31, 2024
Accepted Januari 07, 2024

Keywords:

Siber
Digitalisasi
Manajemen Keamanan
Teknologi

Keywords:

Cyber
Digitalization
Security Management
Technology

ABSTRAK

Manajemen keamanan mencakup seperangkat kebijakan, praktik, dan prosedur yang bertujuan melindungi organisasi dari berbagai ancaman keamanan, termasuk yang berasal dari dunia maya. Fokus utamanya adalah melindungi informasi sensitif dan data penting dari akses, modifikasi, atau penghapusan yang tidak sah. Selain itu, tujuan manajemen keamanan juga melibatkan perlindungan sumber daya teknologi informasi dan komunikasi (TIK) agar tetap aman dan terlindungi. Metode studi literatur digunakan dalam penelitian ini, yang juga menyoroti urgensi manajemen keamanan dalam konteks Dalam konteks era digitalisasi, hasil penelitian menunjukkan bahwa manajemen keamanan merupakan suatu kebutuhan yang sangat penting bagi perusahaan atau organisasi saat ini. Terapannya yang terintegrasi, manajemen risiko yang cermat, dan pelaksanaan kebijakan keamanan yang jelas dapat menjaga informasi keamanan dan teknologi dari potensi serangan dunia maya, sekaligus mengurangi risiko keamanan yang mungkin timbul.

ABSTRACT

Security management encompasses a set of policies, practices, and procedures aimed at protecting an organization from various security threats, including those from cyberspace. The main focus is on protecting sensitive information and critical data from unauthorized access, modification or deletion. In addition, security management objectives also involve protecting information and communication technology (ICT) resources to keep them safe and secure. The literature study method was used in this research, which also highlights the urgency of security management in the context of the digitalization era. The results emphasize that security management is a crucial need for companies or organizations in today's digital age. The implementation of integrated security management, careful risk management, and clear implementation of security policies can safeguard information and technology from cyber attacks and reduce potential security risks. (ukuran 10 pt)

Corresponding Author:

Fried Sinlae
Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya
Jakarta, Indonesia
Email: fried.sinlae@dsn.ubharajaya.ac.id

1. PENDAHULUAN

Saat ini, integrasi teknologi ke dalam kehidupan sehari-hari telah meningkat secara signifikan, menciptakan ancaman keamanan siber yang semakin canggih dan menimbulkan risiko besar bagi organisasi global. Riset menunjukkan bahwa risiko keamanan siber dapat

mengakibatkan kerugian finansial yang besar dan bahkan mengancam kelangsungan hidup organisasi, terutama bagi organisasi kecil dan menengah yang memiliki sumber daya terbatas untuk pulih dari serangan. Meskipun ancaman keamanan siber terus meningkat, banyak organisasi masih kurang memberikan perhatian terhadap manajemen keamanan. Manajemen keamanan informasi mencakup serangkaian kebijakan, praktik, dan prosedur yang dirancang untuk melindungi organisasi dari ancaman keamanan, termasuk serangan dunia maya. Tujuannya adalah untuk melindungi informasi sensitif dan informasi penting dari akses tidak sah, modifikasi, atau penghapusan, serta menjaga keamanan sumber daya teknologi informasi dan komunikasi (TIK) yang digunakan dalam organisasi.

Manajemen informasi keamanan mencakup pengenalan risiko keamanan informasi, pengembangan strategi keamanan yang efektif, dan penerapan praktik dan prosedur keamanan. Penggunaan teknologi keamanan seperti perangkat lunak antivirus, firewall, kata sandi yang kuat, enkripsi, serta kontrol akses pengguna dan pelaporan keamanan rutin juga merupakan bagian integral dari manajemen keamanan. Faktor-faktor yang berkontribusi terhadap kurangnya perhatian terhadap manajemen keamanan informasi termasuk kurangnya kesadaran akan risiko keamanan siber dan terbatasnya sumber daya untuk menerapkan strategi keamanan yang efektif. Perubahan pesat dalam teknologi dan lingkungan bisnis juga menghadirkan tantangan terhadap manajemen informasi keamanan dan mengharuskan organisasi untuk terus memperbarui strategi dan teknik mereka untuk menghadapi ancaman keamanan siber yang terus berkembang.

Dalam konteks ini, latar belakang masalah menyoroti pentingnya manajemen keamanan informasi yang efektif untuk melindungi data sensitif dan informasi penting dari serangan dunia maya, serta untuk meningkatkan operasi dan kepercayaan pelanggan serta pemangku kepentingan lainnya. Latar belakang masalah dan tekanan yang dihadapi organisasi untuk melawan ancaman keamanan menunjukkan perlunya berinvestasi dalam teknologi keamanan dan pelatihan untuk meningkatkan kesadaran keamanan di seluruh organisasi. Oleh karena itu, rumusan soal yang dipertimbangkan meliputi:

1. Peran krusial manajemen keamanan informasi teknologi dalam konteks globalisasi.
2. Dampak sistem teknologi terhadap keamanan informasi perusahaan.
3. Peran sistem manajemen keamanan yang efektif dalam mengatasi ancaman keamanan siber

Tujuan Penelitian

1. Menganalisis signifikansi keamanan informasi teknologi dalam konteks ancaman cyber.
2. Menilai perubahan yang dapat diterapkan pada sistem informasi untuk meningkatkan manajemen keamanan.
3. Mengevaluasi strategi menghadapi tantangan yang muncul dalam keamanan sistem informasi terkait bahaya dan ancaman dalam lingkungan bisnis.
4. Mengidentifikasi langkah-langkah pengurangan risiko yang dapat diterapkan untuk meningkatkan efektivitas kesadaran keamanan.

Dengan tujuan penelitian ini, akan dijelaskan pentingnya keamanan informasi teknologi dalam menghadapi ancaman cyber, modifikasi yang dapat diterapkan pada sistem informasi untuk meningkatkan manajemen keamanan, strategi menghadapi tantangan keamanan sistem

informasi dalam konteks bahaya dan ancaman bisnis, serta langkah-langkah konkrit untuk mengurangi risiko dan meningkatkan kesadaran keamanan secara efektif.

2. METODE

Teknik penelitian kepustakaan adalah teknik penelitian kepustakaan [1]. Hal ini merupakan strategi pengembangan konsep atau teori baru dan menguji konsep atau teori yang sudah ada. Pendekatan ini melibatkan penelitian dan pembelajaran dari berbagai sumber perpustakaan, termasuk buku, jurnal, makalah penelitian, dan bahan lainnya. Pendekatan penelitian kepustakaan diartikan sebagai suatu teknik penelitian yang mengumpulkan, mengkaji dan menyebarkan informasi dari berbagai sumber kepustakaan [2]. Tujuannya untuk memperoleh pemahaman komprehensif terhadap masalah penelitian melalui pemahaman literatur secara komprehensif.

Tabel 1. Hasil Penelitian yang relevan Terdahulu

No	Author (tahun)	Hasil Riset terdahulu	Persamaan dengan artikel ini	Perbedaan dengan artikel ini
1	Melwin Syafrizal [3]	Pengelolaan keamanan informasi diperlukan untuk mendukung pertumbuhan aset. Menurut Menurut survei Bisnis dan Industri Inggris pada tahun 2000, hingga 49% organisasi menganggap informasi sebagai aset yang sangat penting. Hal ini disebabkan oleh potensi pemanfaatan oleh pesaing jika terjadi kebocoran informasi. Selain itu, persentase yang sama, yaitu 49%, menyatakan bahwa keamanan informasi sangat krusial untuk memenangkan kepercayaan pelanggan.	Kedua artikel membahas pentingnya manajemen keamanan dan mengapa manajemen keamanan diperlukan.	Artikel sebelumnya mengeksplorasi manajemen keamanan dengan fokus utama pada standar ISO, sementara artikel ini mengulas aspek manajemen keamanan secara menyeluruh.
2	Tuti Hartati [4]	Aset informasi dari suatu organisasi yang merupakan sistem manajemen yang krusial dapat dijaga dengan melibatkan informasi keamanan. Perlunya keamanan ini muncul untuk menjaga berbagai properti perusahaan, termasuk perangkat lunak, database, file server, media, server, workstation, perangkat keras jaringan, jaringan komunikasi, peningkatan	Keduanya membahas tentang pentingnya manajemen keamanan dalam menjaga kesinambungan.	Artikel sebelumnya memberikan penjelasan yang terfokus pada aspek tertentu, sementara artikel ini membahas topik secara umum.

No	Author (tahun)	Hasil Riset terdahulu	Persamaan dengan artikel ini	Perbedaan dengan artikel ini
		peralatan dan. aset pribadi, sebagaimana telah diungkapkan sebelumnya..		
3	B S Deva, R Jayadi [5]	Berdasarkan pembahasan masalah penelitian, kesimpulan dari hasil wawancara, observasi, dan studi literatur terdapat enam aspek yang perlu diperhatikan karena berpotensi menimbulkan risiko terhadap keamanan informasi. Keenam aspek tersebut mencakup penyebaran atau distribusi data sensitif yang tidak sah, penurunan kinerja fasilitas server, serangan ransomware, serangan malware, kerusakan perangkat seperti laptop, dan kurangnya kesadaran dan pemahaman informasi akan urgensi keamanan.	Kedua artikel membahas aspek-aspek yang memiliki potensi untuk menimbulkan risiko.	Artikel sebelumnya menerapkan pendekatan dengan metode OCTAVE Allegro, sedangkan artikel ini tidak membatasi diri pada metode tertentu selain kerangka kerja penelitian yang digunakan.
4	Bramantiyo Eko Putro [6]	Organisasi harus menerapkan mekanisme audit manajemen keamanan informasi yang disesuaikan dengan persyaratan yang berlaku untuk melindungi perusahaan dari potensi kerugian yang dapat timbul akibat operasi penyimpanan informasi. Dampaknya adalah pertumbuhan dan kompleksitas industri manajemen keamanan informasi.	Kedua artikel membahas tentang keamanan informasi, dengan fokus pada upaya menjaga dari kemungkinan kehilangan data.	Artikel sebelumnya mengeksplorasi topik keamanan informasi dalam kerangka kerja audit, sedangkan artikel ini menjelajahi aspek-aspek keamanan informasi tanpa keterkaitan langsung dengan proses audit.
5	Fitroh et al	Pentingnya faktor keamanan menjadi perhatian utama Dalam penerapan manajemen teknologi, karena efektivitas pengelolaan organisasi dapat dipengaruhi oleh masalah keamanan informasi yang berkaitan dengan kerahasiaan, integritas dan ketersediaan informasi yang merupakan salah satu tujuan	Kedua artikel mengulas beberapa penelitian terdahulu dengan topik serupa.	Implementasi ISO 27001 dalam manajemen keamanan telah dijelaskan secara rinci dalam artikel sebelumnya melalui peninjauan sistematis; Sementara itu, artikel ini hanya memberikan wawasan umum mengenai manajemen keamanan.

No	Author (tahun)	Hasil Riset terdahulu	Persamaan dengan artikel ini	Perbedaan dengan artikel ini
		utama. Untuk mengatasi hal ini, standar keamanan informasi internasional telah diperkenalkan, seperti ISO 27001, yang merupakan sistem manajemen keamanan informasi., menjadi suatu kebutuhan.		
6	Muhammad Bahrudin, Firmansyah [7]	Keberadaan masalah keamanan informasi di dunia maya sangat nyata, sebagaimana terlihat dari statistik di atas. Manajemen perpustakaan perlu mengambil tindakan keamanan atau merencanakan masa depan untuk melindungi aset informasi mereka. Keamanan informasi di dunia maya juga menjadi perhatian, seperti yang tercermin dari data statistik, dan perpustakaan manajemen perlunya mengambil langkah-langkah keamanan informasi atau perencanaan ke depan untuk melindungi aset mereka. Selain itu, diperlukan kerangka kerja untuk manajemen informasi di perpustakaan, termasuk manajemen keamanan informasi.	Artikel kedua membahas mengenai potensi ancaman terhadap keamanan informasi dalam lingkungan cyber.	Artikel sebelumnya membahas analisis keamanan sistem, sedangkan artikel ini tidak membahas aspek analisis keamanan sistem.

3. HASIL DAN PEMBAHASAN

3.1 Peran Penting Manajemen Keamanan Teknologi Informasi

Berdasarkan penelitian sebelumnya, menyimpulkan bahwa pertumbuhan aset memerlukan informasi manajemen keamanan [3]. Survei Bisnis dan Industri Inggris pada tahun 2000 menemukan bahwa 49 persen organisasi menganggap informasi sebagai aset yang begitu penting disebabkan kompetitor mampu mengeksploitasi info yang bocor. Sebanyak 49% organisasi juga menyatakan bahwa keamanan data sangat penting untuk mendapatkan kepercayaan pelanggan. Analisis lebih lanjut dapat dijelaskan dalam beberapa subbagian yang berkaitan dengan bab awal yang dibahas.

Penelitian sebelumnya menunjukkan bahwa sistem manajemen yang krusial Aset informasi pada organisasi, yang mampu dipertahankan dengan langkah-langkah security, mencakup perlindungan terhadap berbagai harta perusahaan misalnya software database, file

server, media storage, server, stasiun kerja, perangkat keras jaringan, jaringan komunikasi, perangkat tambahan peralatan, dan aset pribadi [4]. Dari penelitian sebelumnya bahwa dari hasil wawancara, observasi, dan studi literatur, termasuk identifikasi studi sebelumnya, terdapat enam aspek yang menjadi fokus perhatian karena potensinya dalam menimbulkan risiko keamanan informasi [5]. Keenam aspek tersebut meliputi penyebaran atau penyebaran informasi sensitif yang tidak sah, penurunan fasilitas server, serangan ransomware, serangan malware, kerusakan perangkat seperti laptop, dan kurangnya kesadaran serta pemahaman akan pentingnya keamanan informasi.

Penelitian sebelumnya mencatat perlunya organisasi mengadopsi mekanisme audit manajemen keamanan informasi yang disesuaikan sesuai dengan ketentuan yang berlaku [6]. Langkah ini diambil untuk melindungi perusahaan dari potensi kerugian yang dapat timbul akibat operasi penyimpanan informasi. Dampaknya adalah pertumbuhan dan kompleksitas industri manajemen keamanan informasi. Penelitian lain mencatat bahwa faktor keamanan menjadi penting dalam penerapan tata kelola teknologi kinerja karena organisasi dapat mempengaruhi jika informasi, sebagai salah satu tujuan utama, masalah menghadapi keamanan seperti Keterbukaan, keutuhan, dan ketersediaan informasi. Penerapan standar informasi keamanan internasional seperti ISO 27001 diperlukan untuk mengatasi hal ini. [7] Masalah keamanan informasi di dunia maya adalah nyata dan manajemen perpustakaan harus mengambil langkah-langkah keamanan atau membuat rencana ke depan untuk melindungi aset informasinya. Selain itu, diperlukan kerangka pengelolaan informasi perpustakaan, termasuk pengelolaan keamanan informasi.Secara keseluruhan, hasil penelitian ini menunjukkan bahwa manajemen keamanan informasi sangat penting di era digital saat ini. Organisasi harus menerapkan langkah-langkah keamanan yang efektif, termasuk keamanan berlapis, untuk melindungi data sensitif dan informasi penting dari serangan dunia maya yang semakin canggih dan sering terjadi.

3.2 Sistem Teknologi Mempengaruhi Keamanan Informasi Bagi Perusahaan

Manajemen security informasi yang efektif juga dapat meningkatkan efisiensi operasional organisasi dengan mengurangi waktu dan biaya yang dikeluarkan dalam menanggapi serangan siber dan memulihkan dampak kerusakan yang timbul. Hal ini berpotensi menghemat biaya dan meningkatkan efisiensi seluruh organisasi. Lainnya yaitu pengelolaan keamanan informasi yang efektif juga dapat membangun kepercayaan antara pelanggan dan pihak terkait lainnya. Di era mana keamanan data semakin penting bagi konsumen, organisasi yang mampu menjamin keamanan data yang kuat memiliki potensi untuk meningkatkan loyalitas pelanggan dan memperoleh keunggulan kompetitif yang signifikan.

Namun, hasil penelitian menunjukkan bahwa banyak organisasi, terutama yang berukuran kecil dan menengah, masih belum memberikan perhatian yang memadai terhadap manajemen keamanan. Organisasi-organisasi ini sering berasumsi bahwa ukuran mereka yang relatif kecil membuat mereka kurang rentan terhadap serangan siber. Meskipun demikian, penelitian menunjukkan bahwa organisasi skala kecil dan menengah juga memiliki risiko rentan terhadap serangan saudara, dan dampaknya dapat lebih merugikan karena seringkali mereka kekurangan sumber daya untuk memulihkan serangan tersebut.

Oleh karena itu, penelitian ini menyoroti urgensi peran manajemen dalam memperhatikan keamanan siber dan menerapkan manajemen informasi keamanan yang efektif. Lebih lanjut,

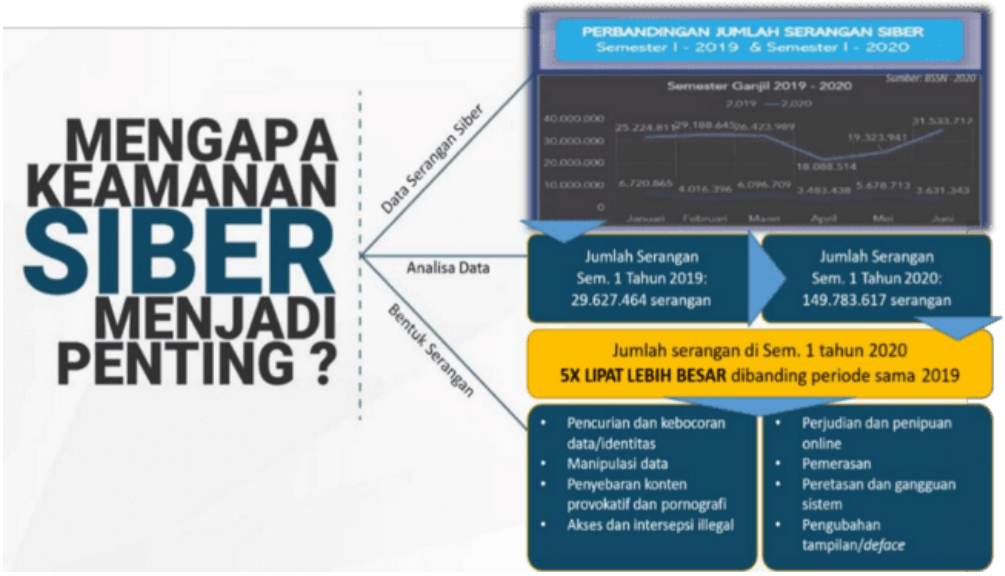
E-ISSN : 3024-8752
P-ISSN : 3024-8744

penelitian menekankan kebutuhan untuk mengalokasikan sumber daya pada teknologi keamanan dan pelatihan untuk meningkatkan kesadaran keamanan di dalam organisasi. Di era digitalisasi yang semakin berkembang, manajemen keamanan informasi yang efektif menjadi kunci untuk kelangsungan hidup dan kesuksesan suatu organisasi. Oleh karena itu, organisasi perlu memberikan prioritas pada manajemen keamanan dan secara terus-menerus memperbarui strategi dan teknik mereka guna menangani ancaman security siber yang semakin rumit dan tidak berubah.

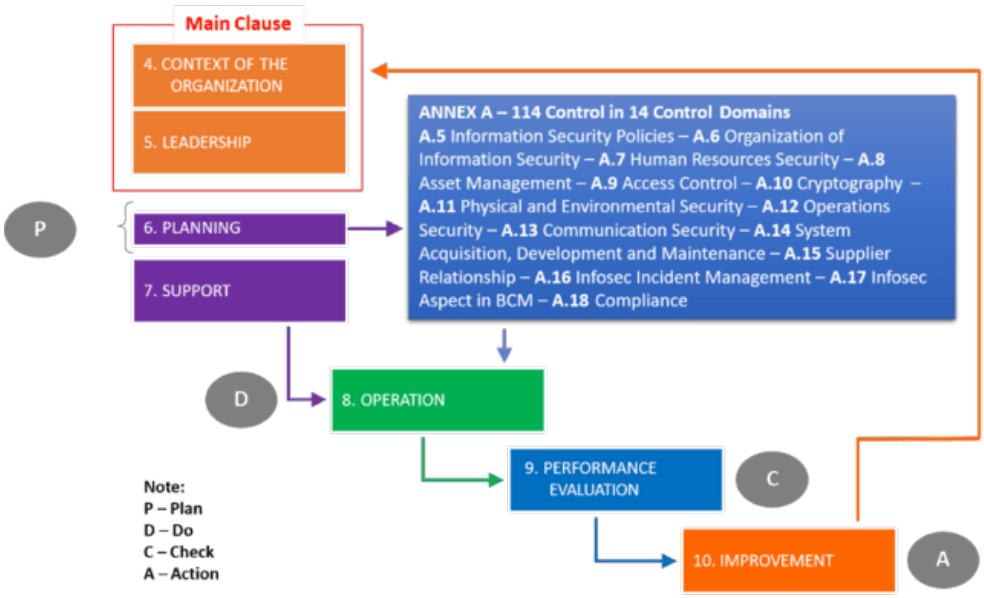
3.3 Peran Sistem Manajemen Keamanan Yang Efektif

Sektor-sektor yang terkait dengan penerapan sangat bergantung pada sistem manajemen keamanan yang efektif (SEMS) selama dekade terakhir. Organisasi di industri transportasi harus mematuhi standar ISO 27001 untuk menerapkan sistem manajemen keselamatan yang efektif dan efisien. Kewajiban legislatif dan persaingan mendorong perusahaan untuk menerapkan sistem manajemen keamanan informasi sesuai standar ISO 27001Tesis doktoral menjelaskan hasil terkait sistem manajemen keamanan informasi. Metode penilaian diri dan pengembangan berkelanjutan menjadi fokus utama penelitian ini. Keselamatan didasarkan pada prinsip dasar European Foundation for Quality Criteria Management (EFQM) dan model Business Excellence.Adanya unsur-unsur yang memerlukan sumber daya organisasi harus secara efektif mendukung keamanan informasi, termasuk aspek-aspek seperti struktur, prosedur, dan sumber daya dalam proses. Tujuan Tietoturva adalah melindungi aset dengan langkah-langkah yang dirancang untuk menjamin kelangsungan bisnis, mengurangi potensi risiko, dan mengoptimalkan laba atas informasi investasi dalam konteks bisnis. Berbagai cara atau taktik dapat diterapkan untuk menciptakan keamanan, dan seringkali cara-cara tersebut digunakan secara bersamaan atau kombinasi. Strategi keamanan dibuat dengan tujuan unik.

3.4 Conceptual Framework



E-ISSN : 3024-8752
P-ISSN : 3024-8744



Gambar 1. Conceptual Framework

4. KESIMPULAN

Di era digitalisasi yang kini tengah berlangsung, manajemen keamanan telah menjadi suatu kebutuhan yang sangat penting bagi perusahaan dan organisasi. Implementasi manajemen keamanan yang terintegrasi, penanganan risiko yang tepat, dan penerapan kebijakan keamanan yang jelas merupakan langkah-langkah esensial yang perlu diambil untuk melindungi informasi dan teknologi yang dimiliki, sehingga dapat meminimalkan potensi risiko serangan siber dan menjaga keamanan secara optimal. Saran untuk penelitian selanjutnya sebaiknya memperinci dan mengkhususkan pembahasan dalam topik serupa dengan penelitian ini. Hal ini dapat melibatkan eksplorasi aspek-aspek spesifik terkait manajemen keamanan, mungkin dengan fokus pada implementasi kebijakan tertentu atau analisis mendalam terhadap strategi penanganan risiko cyber. Dengan demikian, penelitian selanjutnya dapat memberikan kontribusi yang lebih mendalam dan aplikatif dalam memahami serta meningkatkan manajemen keamanan di lingkungan digital.

REFERENSI

[1] Arifin, Z. (2020). Studi Pustaka: Metode Penelitian untuk Menghasilkan Konsep atau Teori Baru. Jurnal Ilmu Pendidikan dan Keguruan, 6(1), 32-40.
[2] Saefudin, A. N., Mulyani, Y., & Fathoni, A. (2021). Penerapan Metode Studi Pustaka dalam Penelitian Hukum Islam. Jurnal Hukum Islam, 5(1), 35-46.
[3] Syafrizal, M. (2009). *Information Security Management System* (ISMS) Menggunakan Standar *ISO/IEC 27001:2005*.
[4] Hartati, T. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013. KOPERTIP: Jurnal Ilmiah Manajemen Informatika dan Komputer, 1(2).
[5] Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan *System Integrator* Menggunakan Metode *Octave Allegro*. Jurnal Teknologi dan Informasi (JATI), 12(2).
[6] Putro, B. E. (2016). Klausul A.5 Analisis Audit Penilaian Mandiri Pengendalian Kebijakan Keamanan Kebijakan pada Klausul A.9 Analisis Audit Penilaian Sendiri Pengendalian

pada Klausul A.9 27001, pengamanan fisik dan lingkungan Telkom Flexi Kebon Sirih Jakarta Pusat. Media Jurnal Informatika, 8(1).

[7] Bahrudin, M., & Firmansyah. (2018). Manajemen Keamanan Informasi di Perpustakaan Menggunakan Framework SNI ISO/IEC 27001. Media Pustakawan, 25(1).