e-ISSN:2829-4580, p-ISSN: 2829-4599
DOI: https://doi.org/10.38035/jim.v2i1
Received: 17 Mei 2023, Revised: 1 Juni 2023, Publish: 2 Juni 2023

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

Pentingnya Manajemen Security di Era Digitalisasi

Rifqi Galuh Putra[1], Achmad Fauzi[2], Ery Teguh Prasetyo[3], Salza Rio Pratama[4], Indah Deya Ramadhan[5], Febriyanti Febriyanti[6], Siti Nurlela[7]
[1.] Universitas Bhayangkara Jakarta Raya, Indonesia, 202010325368@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, 202010325349@mhs.ubharajaya.ac.id
[5.] Universitas Bhayangkara Jakarta Raya, Indonesia, 202010325369@mhs.ubharajaya.ac.id
[6.] Universitas Bhayangkara Jakarta Raya, Indonesia, 202010325351@mhs.ubharajaya.ac.id
[7.] Universitas Bhayangkara Jakarta Raya, Indonesia, 202010325333@mhs.ubharajaya.ac.id

Corresponding Author: Rifqi Galuh Putra

Abstract: *Security management is a set of policies, practices, and procedures designed to protect an organization from security threats, including cyber threats. Its purpose is to protect sensitive information and critical data from unauthorized access, alteration, or deletion, as well as to ensure that information and communication technology (ICT) resources used by organizations are kept safe and secure. This research uses a literature study method. In addition, this research also discusses the importance of security management in the digitalization era. The results of the study explain that security management is a very important requirement for companies or organizations in the current digitalization era. By implementing integrated security management, carrying out appropriate risk management, and implementing clear security policies, companies or organizations can protect their information and technology from cyber-attacks and minimize security risks that may occur.*

Keyword: *Cyber, Digitalization, Security Management, Technology.*

Abstrak: Manajemen keamanan adalah seperangkat kebijakan, praktik, dan prosedur yang dirancang untuk melindungi organisasi dari ancaman keamanan, termasuk ancaman dunia maya. Tujuannya adalah untuk melindungi informasi sensitif dan data penting dari akses, perubahan, atau penghapusan yang tidak sah, serta untuk memastikan bahwa sumber daya teknologi informasi dan komunikasi (TIK) yang digunakan oleh organisasi tetap aman dan terlindungi. Penelitian ini menggunakan metode studi literatur. Selain itu, penelitian ini juga membahas tentang pentingnya manajemen keamanan di era digitalisasi. Hasil penelitian menjelaskan bahwa manajemen keamanan merupakan kebutuhan yang sangat penting bagi perusahaan atau organisasi di era digitalisasi saat ini. Dengan menerapkan manajemen

keamanan terintegrasi, melakukan manajemen risiko yang tepat, dan menerapkan kebijakan keamanan yang jelas, perusahaan atau organisasi dapat melindungi informasi dan teknologinya dari serangan dunia maya dan meminimalkan risiko keamanan yang mungkin terjadi.

Kata Kunci: Siber, Digitalisasi, Manajemen Keamanan, Teknologi.

PENDAHULUAN

Dalam era ini, teknologi semakin terintegrasi dalam kehidupan sehari-hari, sehingga organisasi di seluruh dunia menghadapi ancaman keamanan cyber yang semakin meningkat dan kompleks. Menurut penelitian, ancaman keamanan cyber dapat menyebabkan kerugian finansial yang signifikan bagi organisasi. Dalam beberapa kasus, serangan cyber bahkan dapat mengancam kelangsungan hidup organisasi, terutama bagi organisasi kecil dan menengah yang tidak memiliki sumber daya yang cukup untuk memulihkan diri setelah serangan.

Meskipun risiko keamanan cyber semakin meningkat, masih banyak organisasi yang kurang memperhatikan manajemen keamanan. Manajemen keamanan adalah serangkaian kebijakan, praktik, dan prosedur yang dirancang untuk melindungi organisasi dari ancaman keamanan, termasuk ancaman cyber. Tujuannya adalah untuk melindungi informasi sensitif dan data penting dari akses yang tidak sah, perubahan atau penghapusan, serta untuk memastikan bahwa sumber daya teknologi informasi dan komunikasi (TIK) yang digunakan oleh organisasi tetap aman dan terjaga.

Manajemen keamanan meliputi identifikasi risiko keamanan, pengembangan strategi keamanan yang efektif, dan penerapan kebijakan dan prosedur keamanan. Hal ini melibatkan penggunaan teknologi keamanan seperti perangkat lunak antivirus, firewall, sandi kuat dan enkripsi, serta manajemen akses pengguna dan pelaporan keamanan yang teratur.

Faktor-faktor yang menyebabkan banyak organisasi yang kurang memperhatikan manajemen keamanan, seperti kurangnya kesadaran akan risiko keamanan cyber atau kurangnya sumber daya untuk mengimplementasikan strategi keamanan yang efektif.

Selain itu, perubahan teknologi dan lingkungan bisnis yang semakin cepat juga menimbulkan tantangan bagi manajemen keamanan. Organisasi harus terus memperbarui strategi dan teknik mereka untuk menghadapi ancaman keamanan cyber yang semakin kompleks dan terus berkembang.

Oleh karena itu, latar belakang masalah dalam artikel ini menekankan pentingnya manajemen keamanan yang efektif untuk melindungi informasi sensitif dan data penting dari serangan cyber, serta meningkatkan efisiensi operasional dan memperoleh kepercayaan dari pelanggan dan pemangku kepentingan lainnya. Selain itu, latar belakang masalah juga menyoroti tantangan yang dihadapi oleh organisasi dalam menghadapi ancaman keamanan cyber dan perlunya investasi dalam teknologi keamanan dan pendidikan untuk meningkatkan kesadaran keamanan di seluruh organisasi.

Rumusan Masalah

Sesuai dengan konteks latar belakang yang telah dibahas sebelumnya, beberapa rumusan masalah yang perlu diperhatikan adalah:

1. Apa peran penting manajemen keamanan teknologi informasi di era globalisasi?
2. Bagaimana sistem teknologi mempengaruhi keamanan informasi bagi perusahaan?
3. Apa Peran sistem manajemen keamanan yang efektif?

Tujuan Penelitian

1. Untuk mengetahui seberapa pentingnya cyber dengan keamanan informasi teknologi

2. Untuk mengetahui Memodifikasi sistem informasi yang meningkatkan keamanan manajemen sekuriti
3. Untuk mengetahui baagaimana cara menghadapi tantangan ancaman sistem keamanan dalam bisnis bahaya dan ancaman terhadap keamanan informasi
4. Untuk Mengetahui langkah -langkah pengurangan risiko yang diberlakukan untuk meningkatkan kesadaran keamanan yang efektif

METODE

Teknik studi literatur menurut Arifin (2020) adalah strategi yang digunakan untuk membangkitkan konsep atau teori baru atau menguji konsep atau teori yang sudah ada . Ini melibatkan memeriksa dan mempelajari berbagai sumber perpustakaan , termasuk buku, jurnal, makalah penelitian , dan bahan lainnya .

Sedangkan Menurut Saefudin dkk . (2021) mendefinisikan pendekatan studi literatur sebagai teknik penelitian yang melibatkan pengumpulan , pemeriksaan , dan evaluasi data dari berbagai sumber sastra untuk mendapatkan pemahaman menyeluruh tentang masalah penelitian.

Tabel 1: Hasil Penelitian yang Relevan Terdahulu

No	Author (tahun)	Hasil Riset terdahulu	Persamaan dengan artikel ini	Perbedaan dengan artikel ini
1	Melwin Syafrizal (2009)	Aset tumbuh , memerlukan pengelolaan keamanan informasi. survei yang dilakukan oleh Departemen Perdagangan dan Industri Inggris pada tahun 2000 , 49 % organisasi mengatakan bahwa informasi merupakan aset yang sangat penting karena pesaing dapat memanfaatkan kebocoran informasi , dan 49 % dariorganisasi mengatakan bahwa informasi keamanan sangat penting untuk memenangkan pelanggan.	Kedua artikel membahas pentingnya manajemen keamanan dan mengapa manajemen keamanan diperlukan.	Artikel terdahulu membahas tentang manajemen keamanan yang memiliki topik utama ISO, sedangkan artikel ini membahas tentang manajemen keamanan secara umum.
2	Tuti Hartati (2017)	Sistem manajemen penting adalah aset informasi dari suatu organisasi semua dapat dipertahankan melalui keamanan informasi . keamanan diperlukan untuk melindungi aset perusahaan seperti perangkat lunak, database, dan server file, penyimpanan media, server , dan stasiun kerja , serta perangkat keras jaringan , jaringan komunikasi , perangkat tambahan peralatan, dan	Keduanya membahas tentang pentingnya manajemen keamanan dapat menjaga kesinambungan.	Artikel terdahulu menjelaskan secara spesifik, sedangkan artikel ini membahas secara umum saja.

		aset pribadi , seperti yang telah disebutkan sebelumnya .		
3	B S Deva, R Jayadi (2022)	Sesuai dengan rumusan masalah penelitian, dapat disimpulkan hasil wawancara dan observasi termasuk studi literatur, mengidentifikasi 6 area perhatian yang berpotensi menimbulkan risiko keamanan informasi, yaitu pengungkapan atau penyebaran informasi sensitif yang tidak sah, fasilitas server down, serangan ransomware, serangan malware, kerusakan perangkat seperti laptop, dan kurangnya kesadaran dan pemahaman akan pentingnya keamanan informasi.	Kedua artikel membahas tentang hal yang berpotensi menimbulkan risiko.	Artikel terdahulu menggunakan metode OCTAVE Allegro, sedangkan artikel ini tidak menggunakan metode kecuali metode penelitian.
4	Bramantiyo Eko Putro (2016)	Organisasi memerlukan mekanisme audit manajemen keamanan informasi yang dimodifikasi untuk persyaratan yang berlaku untuk melindungi perusahaan dari potensi kerugian karena operasi penyimpanan informasi telah membuat industri manajemen keamanan informasi menjadi lebih besar dan lebih rumit informasi.	Kedua artikel membahas tentang keamanan informasi menjaga dari kemungkinan kehilangan datanya.	Artikel terdahulu membahas tentang keamanan informasi dalam kaitannya dengan audit, sedangkan artikel ini membahas keamanan informasi tidak dalam kaitannya dengan audit.
5	Fitroh, Tania Nur Hafizah Hersyaf, Muhamad Rizaldi Seputra, Ginanjar Ramadhan, and Ari Nur Rokhman (2017)	Faktor keamanan merupakan hal yang krusial untuk diperhatikan dalam penerapan tata kelola teknologi karena Kinerja kinerja darikelola tata kelola organisasiakan terpengaruh jika informasi , salah satu tujuan utama , menghadapi masalah keamanan informasi akan berkaitan dengan kerahasiaan , integritas , dan ketersediaan informasi .terpengaruh jika informasi, salah satu tujuan utama , menghadapi masalah	Kedua artikel mengulas beberapa penelitian terdahulu dengan topik serupa.	penerapan ISO 27001 di bidang manajemen keamanan dibahas dalam artikel sebelumnya menggunakan tinjauan sistematis ; namun, artikel ini hanya mencakup wawasan manajemen keamanan umum .

		keamanan informasi yang berkaitan dengan kerahasiaan , integritas, dan ketersediaan informasi .Menerapkan standar internasionalkeamanan informasi keamanan informasiISO 27001 , sistem manajemen untuk keamanan informasi , diperlukan untuk mengatasi hal ini.standar ISO 27001, sistem manajemen untuk keamanan informasi , diperlukan untuk mengatasi hal ini. Konsultasi Integral 2013.		
6	Muhammad Bahrudin, Firmansyah (2018)	Masalah keamanan informasikeamanan keprihatinandi dunia maya adalah nyata, seperti yang dapat dilihat dari statistik di atas, dan manajemen perpustakaan harus mengadopsi langkah -langkah keamanan atau rencana ke depan untuk aset informasi mereka .di dunia maya adalah nyata, seperti dapat dilihat dari statistik di atas, dan manajemen perpustakaan harus mengadopsi langkah-langkah keamanan atau rencana ke depan untuk aset informasi mereka . Selain itu, diperlukan kerangka kerja untuk manajemen informasi di perpustakaan , termasuk manajemen keamanan informasi ..	Kedua artikel membahas tentang adanya ancaman keamanan informasi di dunia cyber.	Artikel terdahulu membahas tentang analisis keamanan informasi di sistem, sedangkan artikel ini tidak membahas tentang analisis keamanan informasi di sistem.

HASIL DAN PEMBAHASAN

Peran penting manajemen keamanan teknologi informasi

Melwin Syafrizal (2009) Dari hasil peneliti terdahulu terdapat Aset tumbuh , memerlukan pengelolaan keamanan informasi. survei yang dilakukan oleh Departemen Perdagangan dan Industri Inggris pada tahun 2000 , 49 % organisasi mengatakan bahwa informasi merupakan aset yang sangat penting karena pesaing dapat memanfaatkan kebocoran informasi , dan 49 % dariorganisasi mengatakan bahwa informasi keamanan sangat penting untuk memenangkan pelanggan .

Tuti Hartati (2017) Dari hasil peneliti terdahulu terdapat Sistem manajemen penting adalah aset informasi dari suatu organisasi semua dapat dipertahankan melalui keamanan informasi . keamanan diperlukan untuk melindungi aset perusahaan seperti perangkat lunak,

database, dan server file, penyimpanan media, server , dan stasiun kerja , serta perangkat keras jaringan , jaringan komunikasi , perangkat tambahan peralatan, dan aset pribadi , seperti yang telah disebutkan sebelumnya .

B S Deva, R Jayadi (2022) Dari hasil peneliti terdahulu terdapat Sesuai dengan rumusan masalah penelitian, dapat disimpulkan hasil wawancara dan observasi termasuk studi literatur, mengidentifikasi 6 area perhatian yang berpotensi menimbulkan risiko keamanan informasi, yaitu pengungkapan atau penyebaran informasi sensitif yang tidak sah, fasilitas server down, serangan ransomware, serangan malware, kerusakan perangkat seperti laptop, dan kurangnya kesadaran dan pemahaman akan pentingnya keamanan informasi.

Bramantiyo Eko Putro (2016) Dari hasil peneliti terdahulu terdapat Organisasi memerlukan mekanisme audit manajemen keamanan informasi yang dimodifikasi untuk persyaratan yang berlaku untuk melindungi perusahaan dari potensi kerugian karena operasi penyimpanan informasi telah membuat industri manajemen keamanan informasi menjadi lebih besar dan lebih rumit informasi.

Fitroh, Tania Nur Hafizah Hersyaf, Muhamad Rizaldi Seputra, Ginanjar Ramadhan, and Ari Nur Rokhman (2017) Dari hasil peneliti terdahulu terdapat Faktor keamanan merupakan hal yang krusial untuk diperhatikan dalam penerapan tata kelola teknologi karena Kinerja kinerja darikelola tata kelola organisasiakan terpengaruh jika informasi , salah satu tujuan utama , menghadapi masalah keamanan informasi akan berkaitan dengan kerahasiaan , integritas , dan ketersediaan informasi .terpengaruh jika informasi, salah satu tujuan utama , menghadapi masalah keamanan informasi yang berkaitan dengan kerahasiaan , integritas, dan ketersediaan informasi .Menerapkan standar internasionalkeamanan informasi keamanan informasiISO 27001 , sistem manajemen untuk keamanan informasi , diperlukan untuk mengatasi hal ini.standar ISO 27001, sistem manajemen untuk keamanan informasi , diperlukan untuk mengatasi hal ini. Konsultasi Integral 2013 .

Muhammad Bahrudin, Firmansyah (2018) Dari hasil peneliti terdahulu terdapat Masalah keamanan informasikeamanan keprihatinandi dunia maya adalah nyata, seperti yang dapat dilihat dari statistik di atas, dan manajemen perpustakaan harus mengadopsi langkah - langkah keamanan atau rencana ke depan untuk aset informasi mereka .di dunia maya adalah nyata, seperti dapat dilihat dari statistik di atas, dan manajemen perpustakaan harus mengadopsi langkah-langkah keamanan atau rencana ke depan untuk aset informasi mereka . Selain itu, diperlukan kerangka kerja untuk manajemen informasi di perpustakaan , termasuk manajemen keamanan informasi.

Penelitian menunjukkan bahwa manajemen keamanan menjadi semakin penting di era digitalisasi saat ini. Teknologi semakin terintegrasi dalam kehidupan sehari-hari, sehingga organisasi di seluruh dunia menghadapi ancaman keamanan cyber yang semakin meningkat dan kompleks. Oleh karena itu, perlu adanya manajemen keamanan yang efektif untuk melindungi informasi sensitif dan data penting dari serangan cyber.

Penelitian menunjukkan bahwa organisasi yang menerapkan manajemen keamanan yang tepat dapat mengurangi risiko keamanan cyber dan memperkuat pertahanan mereka terhadap serangan. Salah satu teknik yang dapat digunakan adalah keamanan multilayer, yaitu pendekatan yang melibatkan penggunaan beberapa lapisan perlindungan keamanan, seperti firewall, enkripsi, dan manajemen hak akses.

Sistem teknologi mempengaruhi keamanan informasi bagi perusahaan

Manajemen keamanan yang efektif juga dapat membantu organisasi meningkatkan efisiensi operasional mereka. dilakukan dengan menghabiskan lebih sedikit waktu dan uang untuk bertahan dari serangan dunia maya untuk memperbaiki kerusakan yang mereka lakukan. penghematan biaya dan peningkatan efisiensi organisasi dapat dihasilkan dari ini.

Selain itu, manajemen keamanan yang efektif juga dapat membantu organisasi membangun kepercayaan dari pelanggan dan pemangku kepentingan lainnya. Dalam era di mana keamanan data menjadi semakin penting bagi konsumen, organisasi yang mampu memberikan jaminan keamanan yang kuat dapat meningkatkan loyalitas pelanggan dan memperoleh keuntungan kompetitif yang signifikan.

Namun, penelitian juga menunjukkan bahwa masih banyak organisasi yang kurang memperhatikan manajemen keamanan. Hal ini terutama terjadi pada organisasi kecil dan menengah, yang sering menganggap bahwa mereka tidak menjadi sasaran serangan cyber karena ukuran mereka yang relatif kecil. Padahal, penelitian menunjukkan bahwa organisasi kecil dan menengah juga dapat menjadi sasaran serangan cyber, dan dampaknya bahkan dapat lebih merugikan bagi mereka karena mereka seringkali tidak memiliki sumber daya yang cukup untuk memulihkan diri setelah serangan.

Oleh karena itu, penelitian menekankan pentingnya peran manajemen dalam memperhatikan keamanan cyber dan mengimplementasikan manajemen keamanan yang efektif. Selain itu, penelitian juga menunjukkan pentingnya investasi dalam teknologi keamanan dan pendidikan untuk meningkatkan kesadaran keamanan di seluruh organisasi.

Dalam era digitalisasi yang semakin maju, manajemen keamanan yang efektif menjadi kunci untuk kelangsungan hidup dan kesuksesan organisasi. Oleh karena itu, organisasi harus memprioritaskan manajemen keamanan dan terus memperbarui strategi dan teknik mereka untuk menghadapi ancaman keamanan cyber yang semakin kompleks dan terus berkembang.

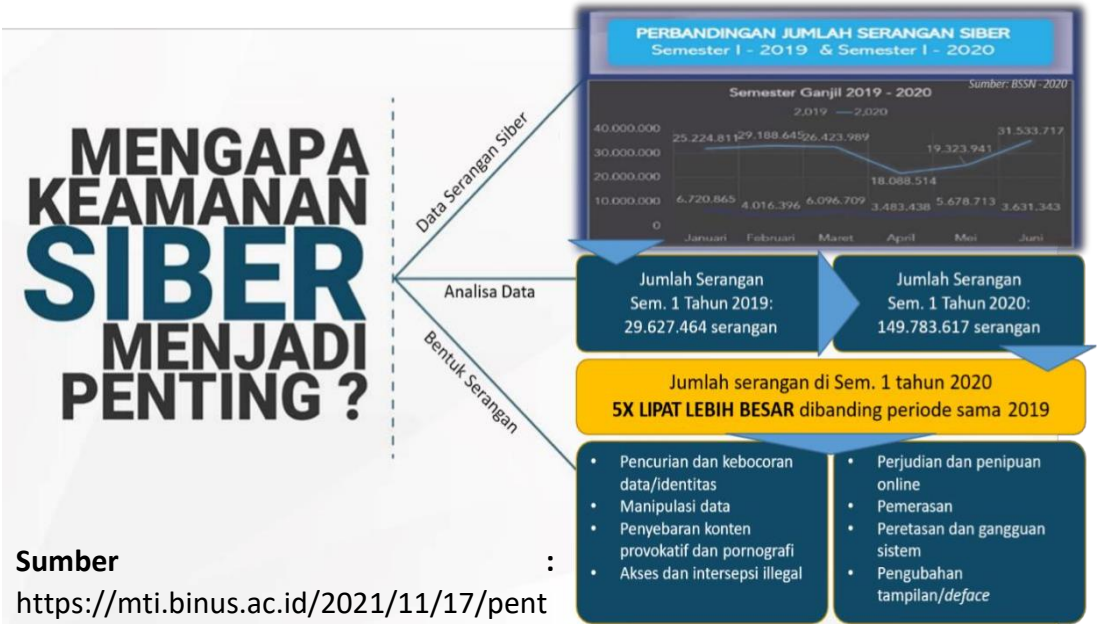
Peran sistem manajemen keamanan yang efektif

Bagi artikel (E, M,& Gram, 2014), industri yang ikut serta dalam industri postingan sangat tergantung pada Sistem Manajemen Keamanan Efektif (SEMS) sepanjang 10 tahun terakhir. Standar ISO 27001 dibutuhkan untuk diperlukan untuk organisasi yang beroperasi di industri transportasi buat menyetujui Sistem Manajemen Keamanan yang Efektif. suatu organisasi yang beroperasi di industri transportasi buat menyetujui Sistem Manajemen Keamanan Efektif dan Efisien. Kewajiban legislatif serta persaingan memusatkan organisasi buat mengadopsi Sistem Manajemen Keamanan yang cocok dengan standar ISO 27001. Organisasi buat mengadopsi Sistem Manajemen Keamanan yang cocok denganstandar ISO 27001 standar.

Publikasi (Hohana, Olarub, Ionela,& Pirneac, 2015), sebagian temuanPenelitian PhD tentang sistem manajemen keamanan data sudah ditekankan. Tata cara methods for penilaian diri serta self- evaluation berkepanjangan merupakan topik utama dari riset ini. and ongoing development are the main topics of this study. Keamanan bersumber pada ilham fundamental serta Model Keunggulan Bisnis dari Yayasan Eropa buat Manajemen Kriteria Mutu(EFQM).

Keberadaan item - item berikut yang akan diselidiki harus mendukung keamanan informasi, antara lain keberadaan item berikut untuk diselidiki harus mendukung keamanan informasi, termasuk: struktur, dan prosedur dan sumber daya proses tujuan keamanan informasi adalah untuk melindungi aset informasi yang dimiliki langkah-langkah dirancang untuk menjamin kelangsungan perusahaan , mengurangi potensi risiko , dan mengoptimalkan pengembalian investasi prospek komersial . berbagai metode atau taktik yang dapat digunakan untuk membangun keamanan , dan ini biasanya digunakan bersama -sama atau dalam kombinasi dengan satu sama lain. strategi keamanan memiliki tujuan yang unik dan dibangun dengan mempertimbangkan tujuan tersebut .

Conceptual Framework



Sumber : https://mti.binus.ac.id/2021/11/17/pentingnya-iso-27001-sebagai-standard-

Gambar 1: Conceptual Framework

Sesuai figure, maka dapat diketahui bahwa manajemen keamanan penting karena terdapat banyak serangan keamanan informasi dari tahun ke tahun dengan berbagai bentuk serangan.

KESIMPULAN

Manajemen keamanan menjadi suatu kebutuhan yang sangat penting bagi perusahaan atau organisasi di era digitalisasi saat ini. Dengan menerapkan manajemen keamanan yang terintegrasi, melakukan penanganan risiko yang tepat, dan menjalankan kebijakan keamanan yang jelas, perusahaan atau organisasi dapat melindungi informasi dan teknologi yang dimilikinya dari serangan cyber dan meminimalkan risiko keamanan yang mungkin terjadi.

Saran untuk penelitian selanjutnya dapat ditambahkan lebih rinci dan spesifik mengenai pembahasan dalam topik serupa dengan penelitian ini.

REFERENSI

Arifin, Z. (2020). Studi Pustaka: Metode Penelitian untuk Menghasilkan Konsep atau Teori Baru. Jurnal Ilmu Pendidikan dan Keguruan, 6(1), 32-40.

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

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).

Dwi Nugraheni, D., & Santoso, D. (2020). Analisis Manajemen Keamanan Sistem Informasi Dalam Meningkatkan Kinerja Perusahaan. Jurnal Sains dan Teknologi Informasi (JUSTIN), 2(2), 72-80.

Genaldo, R., Septyawan, T., Surahman, A., & Prasetyawan, P. (2020). Sistem Keamanan pada Ruangan Pribadi Menggunakan Mikrokontroler Arduino dan SMS Gateway. Jurnal Teknik dan Sistem Komputer (JTIKOM), 1(2).

Hartati, T. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013. KOPERTIP: Jurnal Ilmiah Manajemen Informatika dan Komputer, 1(2).

Nursam, N. (2017). Manajemen Kinerja. Kelola, 2(2).

N. Nursam (2017). Penerapan ISO 27001 dalam pengelolaan risiko mensyaratkan _membutuhkan tinjauan sistemik tinjauan sistemik . Seminar Nasional Sains dan Seminar Teknologi

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.

Syafrizal, M. (2009). Information Security Management System (ISMS) Menggunakan Standar ISO/IEC 27001:2005.