Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 4, Issue June, 2026 pp. 489-496 http://urj.uin-malang.ac.id/index.php/mij/index

Peran manajemen risiko dalam menghadapi ancaman siber di era digital

Reki Ahmad
Program Studi Perbankan Syariah, Universitas Islam Negeri Mulana Malik Ibrahim Malang
e-mail: 230503110088@student.uin-malang.ac.id

Kata Kunci:
Manajemen risiko, keamanan siber, ancaman siber, era digital, ISO 27001, NIST.

Keywords:
Risk management, cybersecurity, cyber threats, digital era, ISO 27001, NIST.

A B S T R A K

Meskipun kemajuan teknologi digital yang pesat telah membuat banyak tugas organisasi lebih mudah, mereka juga lebih rentan terhadap ancaman siber seperti peretasan, pencurian data, dan serangan malware. Untuk menjaga keamanan informasi dan keberlanjutan operasional, organisasi harus memiliki sistem pengelolaan risiko yang kuat karena kondisi ini. Tujuan dari penelitian ini adalah untuk melihat bagaimana manajemen risiko berperan dalam menghadapi ancaman siber di era digital. Penelitian ini menggunakan metodologi kualitatif dan melakukan penelitian literatur terkait. Hasilnya menunjukkan bahwa manajemen risiko sangat penting untuk mengidentifikasi, menganalisis, dan memitigasi ancaman siber potensial melalui penerapan kebijakan keamanan, penggunaan teknologi pendukung, dan peningkatan kesadaran sumber daya manusia. Selain itu, penerapan kerangka kerja seperti ISO 27001 dan NIST Cybersecurity Framework terbukti mampu meningkatkan efektivitas pengelolaan risiko siber dalam organisasi. Dengan demikian, implementasi manajemen risiko yang terintegrasi menjadi kunci utama dalam menghadapi dinamika ancaman siber di era digital.

A B S T R A C T

Even though advanced digital technology has made many organisational tasks easier, they are also more vulnerable to cyber threats like malware, data breaches, and peretasan. Because of this situation, organisations need to have a strong risk management system in order to protect information security and operational efficiency. The purpose of this study is to examine how risk management is effective in dealing with cyber threats in the digital age. This research employs a qualitative methodology and does related literary analysis. The results indicate that risk management is crucial for identifying, analysing, and mitigating potential threats through the implementation of safety regulations, the use of pendukung technology, and the enhancement of human sumber daya. Furthermore, the application of frameworks such as ISO 27001 and the NIST Cybersecurity Framework has proven to improve the effectiveness of cyber risk management within organizations. Therefore, the implementation of integrated risk management is a key factor in dealing with the dynamics of cyber threats in the digital era.

Pendahuluan

Perkembangan teknologi digital yang berlangsung sangat cepat telah membawa perubahan besar dalam berbagai aspek kehidupan, khususnya pada aktivitas organisasi dan bisnis. Transformasi digital memberikan kemudahan melalui proses kerja yang lebih efektif, cepat, dan terintegrasi. Namun, kemajuan tersebut juga diiringi dengan

munculnya berbagai ancaman terhadap keamanan informasi yang semakin kompleks. Risiko seperti peretasan (*hacking*), kebocoran data (*data breach*), hingga penyebaran malware dapat mengganggu stabilitas operasional organisasi dan menimbulkan kerugian yang signifikan

Ancaman siber bukan saja menyebabkan pada kerugian keuangan, melainkan juga mampu menghancurkan kredibilitas organisasi serta mengurangi tanggapan publik. Pada situasi tersebut, keselamatan informasi yaitu sangat krusial untuk diperhatikan. Menurut (Siregar & Mardiah, 2025), perlindungan terhadap data dan sistem informasi harus menjadi prioritas utama karena kebocoran data dapat menyebabkan dampak jangka panjang yang merugikan organisasi, baik dari segi ekonomi maupun kepercayaan stakeholder. Hal tersebut diperkuat oleh (Prakasa, 2020) yang menjelaskan bahwa meningkatnya variasi dan pola serangan terhadap sistem informasi menunjukkan pentingnya peningkatan keamanan sistem sebagai upaya perlindungan terhadap data dan infrastruktur digital organisasi

Semakin kompleksnya ancaman siber di era digital menuntut organisasi untuk tidak hanya bergantung pada penggunaan teknologi keamanan semata, tetapi juga menerapkan manajemen risiko secara terstruktur. Proses ini mencakup identifikasi, analisis, evaluasi, hingga pengendalian risiko yang berpotensi menghambat tercapainya tujuan organisasi (Ramadhanty, 2024). Dalam penerapannya, manajemen risiko keamanan informasi berfungsi sebagai pedoman bagi organisasi dalam mengenali tingkat kerentanan sistem serta menentukan langkah mitigasi yang sesuai guna menjaga keamanan data dan keberlangsungan operasional (Hariyadi & Prakasa, 2023).

Penerapan kerangka kerja internasional seperti ISO 27001 dan NIST Cybersecurity Framework menjadi bagian dari strategi yang secara luas digunakan dalam mengelola risiko siber. Kedua standar tersebut menyediakan panduan komprehensif dalam mengidentifikasi aset, menilai ancaman, serta mengimplementasikan kontrol keamanan yang efektif (Alam et al., 2025). Adanya standar ini memungkinkan organisasi untuk memperkuat pertahanan mereka terhadap serangan siber yang terus berkembang.

Penelitian ini bertujuan untuk menganalisis peran risiko manajemen dalam menangani ancaman siber di era digital dengan mempertimbangkan latar belakang ini. Rumusan masalah penelitian ini adalah bagaimana manajemen risiko dapat membantu organisasi dalam mengidentifikasi, mengendalikan, dan memitigasi ancaman siber. Oleh karena itu, diharapkan penelitian ini akan memberikan pemahaman yang lebih baik tentang seberapa pentingnya penerapan manajemen risiko sebagai strategi pencegahan ancaman terkini .

Pembahasan

Jenis dan Sumber Risiko Siber

Pada era digital saat ini, risiko siber menjadi salah satu ancaman utama yang dihadapi oleh organisasi. Efek tersebut mampu berawal dari berbagai sumber, misal internal maupun eksternal, serta dipengaruhi oleh faktor teknologi dan operasional. Pemahaman terhadap jenis dan sumber risiko siber menjadi langkah awal yang penting dalam penerapan manajemen risiko yang efektif.

Risiko internal merupakan ancaman yang berasal dari dalam organisasi itu sendiri, terutama yang disebabkan oleh sumber daya manusia. Salah satu bentuk risiko internal yang paling umum adalah human error, seperti kesalahan dalam pengelolaan sistem, penggunaan password yang lemah, atau kelalaian dalam menjaga kerahasiaan data. Selain itu, kurangnya kesadaran dan pelatihan terkait keamanan siber juga dapat meningkatkan potensi terjadinya pelanggaran keamanan. Menurut (Tan & Soewito, 2022), sebagian besar insiden keamanan informasi disebabkan oleh faktor internal, terutama karena kurangnya pemahaman terhadap prosedur keamanan yang berlaku.

Risiko eksternal berasal dari pihak luar organisasi, seperti hacker, kelompok kriminal siber, maupun serangan yang terorganisir. Ancaman ini umumnya dilakukan dengan tujuan mencuri data, merusak sistem, atau memperoleh keuntungan finansial. Bentuk serangan yang sering terjadi antara lain phishing, ransomware, dan distributed denial of service (DDoS). (Siregar & Mardiah, 2025), menyatakan bahwa perkembangan teknologi digital telah mempermudah pelaku kejahatan siber dalam melancarkan aksinya, sehingga organisasi harus terus mengembangkan pola peenjagaan dengan makin canggih serta fleksibel.

Risiko teknologi berkaitan dengan kelemahan atau kerentanan pada sistem informasi dan infrastruktur teknologi yang digunakan oleh organisasi. Hal ini dapat meliputi penggunaan perangkat lunak yang tidak diperbarui (outdated software), sistem yang tidak memiliki perlindungan memadai, serta celah keamanan (security vulnerabilities) yang belum ditangani. Kerentanan yang mampu mengambil tindakan oleh individu yang tidak bertanggung jawab untuk mengakses sistem secara ilegal. Menurut (Hafid, 2019), kelemahan dalam sistem teknologi merupakan salah satu faktor utama terjadinya kebocoran data dan gangguan operasional.

Risiko siber juga dapat berdampak pada aspek operasional dan reputasi organisasi. Gangguan pada sistem akibat serangan siber dapat menyebabkan terhentinya aktivitas bisnis, kehilangan data penting, serta kerugian finansial yang signifikan. Selain itu, insiden keamanan siber dapat merusak citra organisasi di mata publik dan menurunkan tingkat kepercayaan pelanggan. (Tan & Soewito, 2022), menjelaskan bahwa dampak reputasi dari serangan siber sering kali lebih besar dibandingkan kerugian finansial, karena berkaitan dengan kepercayaan jangka panjang stakeholder terhadap organisasi.

Peran Manajemen Risiko dalam Menghadapi Ancaman Siber

Dalam menghadapi meningkatnya ancaman siber di era digital, manajemen risiko memiliki peran yang sangat strategis dalam membantu organisasi mengidentifikasi, menganalisis, serta mengendalikan potensi risiko yang dapat mengganggu keamanan informasi dan keberlangsungan operasional. Penerapan manajemen risiko yang sistematis memungkinkan organisasi pada akhirnya terus menyusuri berbagai bentuk serangan siber dengan semakin menyebar

Langkah awal dalam manajemen risiko adalah melakukan identifikasi terhadap seluruh potensi ancaman siber yang mungkin terjadi. Proses ini melibatkan pengenalan aset penting organisasi, seperti data, sistem informasi, serta infrastruktur teknologi yang rentan terhadap serangan. Dengan melakukan pemetaan risiko, organisasi dapat

mengetahui titik-titik lemah yang berpotensi menjadi sasaran serangan. Menurut (Aprianti et al., 2023), proses identifikasi risiko merupakan tahap krusial dalam kerangka kerja manajemen risiko karena menjadi dasar dalam menentukan langkah pengendalian yang tepat.

Setelah risiko diidentifikasi, langkah selanjutnya adalah melakukan analisis dan evaluasi terhadap tingkat risiko tersebut. Penelitian dilaksanakan untuk mengetahui kemungkinan terjadinya risiko (likelihood) serta dampak yang ditimbulkan (impact). Hasil analisis ini kemudian digunakan untuk menentukan prioritas penanganan risiko. (Ramadhanty, 2024) menyatakan bahwa evaluasi risiko membantu organisasi dalam mengalokasikan sumber daya secara efektif dengan fokus pada risiko yang memiliki tingkat dampak paling besar.

Peran penting manajemen risiko selanjutnya adalah merancang dan menerapkan strategi mitigasi dalam mengecilkan maupun mengendalikan risiko yang telah diidentifikasi. Strategi ini dapat berupa penggunaan teknologi keamanan seperti firewall, enkripsi data, sistem deteksi intrusi (intrusion detection system), serta pencadangan data (backup system). Selain itu, organisasi juga perlu menyusun rencana penanganan insiden (incident response plan) untuk meminimalkan dampak jika terjadi serangan. Putri et al. (2025) menjelaskan bahwa penerapan kontrol keamanan yang tepat dapat secara signifikan menurunkan tingkat kerentanan sistem terhadap ancaman siber.

Manajemen risiko juga berperan dalam menyusun kebijakan dan prosedur keamanan yang jelas dan terstruktur. Kebijakan ini mencakup aturan penggunaan sistem, pengelolaan akses, serta standar operasional dalam menjaga keamanan informasi. Penerapan standar internasional seperti ISO 27001 menjadi salah satu bentuk implementasi kebijakan yang efektif dalam mengelola keamanan informasi. Menurut (Resta et al., 2025), organisasi yang menerapkan kebijakan keamanan berbasis standar internasional cenderung memiliki tingkat kesiapan yang lebih tinggi dalam menghadapi ancaman siber.

Faktor manusia menjadi salah satu komponen penting dalam menjaga keamanan siber di lingkungan organisasi. Oleh karena itu, penerapan manajemen risiko perlu disertai dengan upaya edukasi dan peningkatan kesadaran sumber daya manusia mengenai pentingnya perlindungan informasi. Pelatihan secara rutin terkait praktik keamanan digital, seperti mengenali email phishing, menghindari tautan mencurigakan, serta penggunaan kata sandi yang kuat, dapat membantu mengurangi risiko akibat kesalahan pengguna. (Iskandar et al., 2025) menjelaskan bahwa kemampuan literasi digital memiliki hubungan yang erat dengan tingkat kesadaran keamanan siber, sehingga peningkatan pemahaman pengguna menjadi langkah preventif yang efektif dalam meminimalkan insiden keamanan informasi

Faktor manusia menjadi salah satu aspek yang sangat menentukan dalam menjaga keamanan siber di lingkungan organisasi. Oleh sebab itu, penerapan manajemen risiko tidak hanya berfokus pada teknologi, tetapi juga perlu disertai dengan peningkatan pengetahuan dan kesadaran sumber daya manusia mengenai pentingnya perlindungan informasi. Upaya tersebut dapat dilakukan melalui pelatihan keamanan secara berkala,

seperti edukasi mengenai bahaya phishing, penggunaan kata sandi yang aman, serta tata cara penggunaan sistem digital yang benar. Menurut (Wicaksono, 2022), peningkatan kesadaran karyawan merupakan langkah preventif yang efektif untuk meminimalkan terjadinya insiden keamanan siber. Selain itu, (Iskandar et al., 2025) menjelaskan bahwa literasi digital dan pemahaman keamanan siber menjadi faktor penting dalam membangun budaya keamanan informasi di era transformasi digital

Peran terakhir dari manajemen risiko adalah melakukan monitoring dan evaluasi secara berkelanjutan terhadap sistem keamanan yang telah diterapkan. Hal ini penting karena ancaman siber terus berkembang seiring dengan kemajuan teknologi. Dengan adanya proses pemantauan yang rutin, organisasi dapat mendeteksi potensi ancaman lebih dini dan melakukan perbaikan sistem secara cepat. (Ramadhanty, 2024) menyatakan bahwa evaluasi berkelanjutan merupakan kunci dalam menjaga efektivitas manajemen risiko siber dalam jangka panjang.

Strategi dan Implementasi

Dalam menghadapi ancaman siber yang semakin kompleks, organisasi perlu merancang strategi yang tepat serta mengimplementasikan manajemen risiko secara efektif dan terintegrasi. Strategi dan implementasi ini tidak hanya berfokus pada penggunaan teknologi, tetapi juga mencakup aspek kebijakan, sumber daya manusia, serta dukungan manajerial yang kuat.

Strategi utama dalam menghadapi risiko siber adalah mengintegrasikan manajemen risiko ke dalam sistem teknologi informasi organisasi. Hal ini dilakukan dengan memastikan bahwa setiap proses bisnis yang berbasis digital telah melalui analisis risiko dan memiliki kontrol keamanan yang memadai. Integrasi ini memungkinkan organisasi untuk secara proaktif mengidentifikasi potensi ancaman serta meresponsnya dengan cepat. (Kholidah, 2021) menjelaskan bahwa penerapan manajemen risiko berbasis sistem informasi dapat meningkatkan efektivitas pengendalian risiko serta meminimalkan potensi gangguan operasional.

Implementasi strategi keamanan juga melibatkan penggunaan bermacam-macam rekayasa pendukung, seperti firewall, mengolah data, antivirus, serta prosedur deteksi dan pencegahan intrusi (intrusion detection and prevention systems). Selain itu, perkembangan teknologi seperti kecerdasan buatan (*Artificial Intelligence*/AI) juga mulai dimanfaatkan untuk mendeteksi pola serangan siber secara lebih cepat dan akurat. Menurut (Resta et al., 2025), penggunaan teknologi keamanan yang tepat dapat meningkatkan kemampuan organisasi dalam mendeteksi dan mencegah serangan siber secara real-time.

Strategi lain yang penting adalah mengadopsi standar dan kerangka kerja internasional dalam pengelolaan keamanan informasi, seperti ISO 27001 dan NIST Cybersecurity Framework. Standar ini menyediakan panduan sistematis dalam mengidentifikasi, menganalisis, serta mengendalikan risiko siber. Dengan menerapkan standar tersebut, organisasi dapat meningkatkan kualitas sistem keamanan serta memastikan kesesuaian dengan praktik terbaik (best practices) secara global. (Alam et al., 2025)menyatakan bahwa organisasi yang mengadopsi standar internasional cenderung memiliki sistem keamanan yang lebih terstruktur dan efektif.

Keberhasilan implementasi manajemen risiko siber sangat bergantung pada dukungan dari manajemen puncak. Pimpinan organisasi memiliki peran penting dalam menetapkan kebijakan, menyediakan sumber daya, serta memastikan bahwa strategi keamanan dijalankan secara konsisten. Tanpa komitmen dari manajemen, implementasi manajemen risiko tidak akan berjalan optimal. (Aprianti et al., 2023) menegaskan bahwa keterlibatan manajemen puncak menjadi faktor kunci dalam keberhasilan penerapan sistem manajemen keamanan informasi.

Pada praktiknya, banyak institut telah mengerjakan tata kelola anacaman siber untuk menghadapi intimidasi digital. Diantara contoh adalah instansi pemerintah yang menggunakan pendekatan berbasis NIST untuk mengidentifikasi aset, menilai tingkat risiko, dan menentukan prioritas mitigasi. Hasil analisis menunjukkan adanya klasifikasi risiko menjadi tingkat tinggi, sedang, dan rendah, sehingga memudahkan organisasi dalam menentukan langkah penanganan yang tepat. (Resta et al., 2025) menunjukkan bahwa pendekatan berbasis risiko ini mampu meningkatkan kesiapan organisasi dalam menghadapi berbagai potensi serangan siber.

Tantangan dalam Manajemen Risiko Siber

Dalam penerapan manajemen risiko siber, organisasi tidak hanya dihadapkan pada kebutuhan untuk mengidentifikasi dan mengelola risiko, tetapi juga berbagai tantangan yang dapat menghambat efektivitas implementasinya. Tantangan ini muncul seiring dengan perkembangan teknologi yang cepat, keterbatasan sumber daya, serta kompleksitas sistem digital yang semakin tinggi

Salah satu tantangan utama dalam manajemen risiko siber adalah pesatnya perkembangan teknologi digital. Inovasi seperti cloud computing, Internet of Things (IoT), dan kecerdasan buatan (AI) membawa manfaat besar, namun juga menciptakan celah keamanan baru yang sulit diprediksi. Ancaman siber berkembang seiring dengan teknologi yang digunakan, sehingga organisasi harus terus memperbarui sistem keamanan dan strategi mitigasi risiko. (Resta et al., 2025) menyatakan bahwa dinamika perkembangan teknologi menyebabkan pendekatan keamanan konvensional menjadi kurang efektif jika tidak diimbangi dengan inovasi yang berkelanjutan.

Selain itu, tantangan berikutnya adalah rendahnya tingkat kesadaran dan literasi keamanan siber, terutama di kalangan sumber daya manusia. Banyak insiden keamanan terjadi akibat kelalaian pengguna, seperti membuka email phishing, menggunakan kata sandi yang lemah, atau tidak mengikuti prosedur keamanan yang telah ditetapkan. (Mahendra & Soewito, 2023)menjelaskan bahwa kurangnya pemahaman tentang keamanan informasi menjadi faktor dominan dalam terjadinya pelanggaran sistem, sehingga edukasi dan pelatihan menjadi hal yang sangat penting.

Di satu sisi, sebagian besar instansi mempunyai permulaan potensi itu cukup untuk menjalankan manajemen risiko siber secara optimal. Keterbatasan tenaga ahli di bidang keamanan siber serta biaya investasi yang cukup besar untuk teknologi keamanan menjadi kendala utama, khususnya bagi organisasi kecil dan menengah. (Ramadhanty, 2024) menyebutkan bahwa kurangnya alokasi sumber daya dapat menghambat penerapan sistem keamanan yang komprehensif dan berkelanjutan.

Seiring dengan digitalisasi yang semakin luas, sistem informasi organisasi menjadi semakin kompleks dan terintegrasi. Kompleksitas ini mencakup penggunaan berbagai platform, aplikasi, serta jaringan yang saling terhubung, sehingga meningkatkan potensi terjadinya celah keamanan. Selain itu, integrasi sistem lama (*legacy systems*) dengan teknologi baru juga dapat menimbulkan risiko tambahan. (Resta et al., 2025) menegaskan bahwa semakin kompleks sistem yang digunakan, semakin tinggi pula tingkat kerentanan terhadap serangan siber.

Tantangan lainnya adalah belum meratanya penerapan standar keamanan informasi di berbagai organisasi. Tidak semua organisasi mengadopsi kerangka kerja seperti ISO 27001 atau NIST Cybersecurity Framework, sehingga pengelolaan risiko sering kali dilakukan secara tidak terstruktur. (Mahendra & Soewito, 2023) menyatakan bahwa kurangnya standarisasi dan kepatuhan terhadap regulasi dapat meningkatkan potensi risiko serta memperlemah sistem pertahanan terhadap ancaman siber.

Kesimpulan dan Saran

Berdasarkan keseluruhan diskusi tentang peran manajemen risiko dalam menghadapi ancaman siber di era digital, dapat disimpulkan bahwa pertumbuhan teknologi yang semakin pesat telah memberikan pertukaran luar bisa terhadap beragam kacamata gerakan organisasi, terutama dalam hal penggunaan sistem informasi dan teknologi digital. Meskipun transformasi digital membawa beberapa keuntungan, transformasi digital juga membawa berbagai ancaman siber yang semakin kompleks, seperti peretasan dan pencurian data. Faktor-faktor internal, seperti kesalahan manusia, kurangnya kesadaran keamanan, dan kelemahan sistem teknologi yang digunakan, merupakan sumber risiko tersebut. Faktor-faktor eksternal, seperti hacker dan pihak yang tidak bertanggung jawab, juga termasuk. Dalam situasi seperti ini, manajemen risiko menjadi bagian penting dari menjaga keamanan informasi dan keberlangsungan operasi organisasi.

Melalui proses yang sistematis, yaitu identifikasi, analisis, evaluasi, dan mitigasi risiko, organisasi dapat memahami potensi ancaman yang dihadapi serta menentukan langkah penanganan yang tepat dan efektif. Selain itu, penerapan strategi yang terintegrasi, seperti pemanfaatan teknologi keamanan, penerapan kebijakan dan prosedur yang jelas, serta adopsi standar internasional seperti ISO 27001 dan NIST Cybersecurity Framework, terbukti mampu meningkatkan ketahanan organisasi terhadap ancaman siber. Namun, berbagai tantangan masih ada dalam penerapannya, termasuk kemajuan teknologi yang pesat, keterbatasan sumber daya manusia dan keuangan, rendahnya kesadaran tentang keamanan siber, dan meningkatnya kompleksitas sistem digital. Oleh karena itu, komitmen yang kuat dari semua pemangku kepentingan organisasi sangat penting untuk pelaksanaan manajemen risiko yang konsisten dan berkelanjutan.

Sejalan dengan kesimpulan tersebut, disarankan agar organisasi meningkatkan penerapan manajemen risiko siber secara lebih terstruktur dan terintegrasi dengan sistem teknologi informasi yang digunakan. Selain itu, penting untuk melakukan investasi dalam teknologi keamanan yang memadai serta meningkatkan kapasitas

sumber daya manusia melalui pelatihan dan edukasi terkait keamanan siber. Penguatan kebijakan dan prosedur internal juga perlu dilakukan agar setiap aktivitas digital berjalan sesuai dengan standar keamanan yang telah ditetapkan. Selain itu, untuk meningkatkan efisiensi pengelolaan risiko, organisasi harus mengadopsi dan menerapkan standar internasional seperti ISO 27001 dan NIST Cybersecurity Framework. Sebaliknya, untuk memberikan kontribusi yang lebih spesifik, penelitian selanjutnya diharapkan dapat mempelajari lebih lanjut bagaimana manajemen risiko dapat diterapkan pada sektor-sektor tertentu . Dengan mengambil tindakan ini, organisasi yang diharapkan dapat lebih siap menghadapi ancaman siber yang berkembang, bahkan bisa merawat operasional beserta keamanan data di era digital .

Daftar Pustaka

Alam, R. G., Hidayah, A. K., Gunawan, G., Wijaya, A., & Abdullah, D. (2025). Manajemen Risiko Keamanan Informasi. PT. Sonpedia Publishing Indonesia.

Aprianti, S., Sari, R. P., & Rusi, I. (2023). Manajemen Risiko Keamanan Simbada Menggunakan Metode NIST SP 800-30 Revisi 1 dan Kontrol ISO / IEC 27001: 2013. 14(April), 50–59.

Hafid, M. H. (2019). Investigasi Log Jaringan Untuk Deteksi Serangan Distributed Denial Of Service (DDOS) Dengan Menggunakan Metode General Regression Neural Network.

Hariyadi, M. A., & Prakasa, J. E. W. (2023). Manajemen Keamanan Sistem Informasi. UIN Maliki Press. https://repository.uin-malang.ac.id/17952

Iskandar, I., Putra, D. D., Yasin, A. I., & Khairan, K. (2025). Cyber Smart Campus: Cakap Digital & Aman Siber. PT. Sonpedia Publishing Indonesia. https://repository.uin-malang.ac.id/25350

Kholidah, M. (2021). Manajemen Layanan Perpustakaan Berbasis Teknologi Informasi Sebagai Pendukung Pembelajaran Pemustaka (Studi Kasus Perpustakaan Uin Maulana Malik Ibrahim Malang).

Mahendra, V., & Soewito, B. (2023). Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber. Techno. Com, 22(3).

Prakasa, J. E. W. (2020). Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi. Jurnal Ilmiah Teknologi Informasi Asia, 14(2), 75–84. https://repository.uin-malang.ac.id/5506/

Ramadhanty, N. (2024). Implementasi Kerangka Keamanan NIST Dan ISO / IEC 27001 Dalam Menghadapi Ancaman Risiko Siber. (4), 1–9.

Resta, S., Putri, M., Bernandy, M. P., Aulia, C., Ghaza, M., Fikri, R., Jasmine, J., & Surabaya, U. N. (2025). Indonesian Journal of Digital Business Praktik Manajemen Resiko Keamanan Siber: Wawasan Dari Organisasi Bersertifikat ISO 27001. 5(April), 1–10.

Siregar & Mardiah. (2025). Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO / IEC 27001. 1(2), 58–64.

Tan, T., & Soewito, B. (2022). Menggunakan Framework NIST Cybersecurity di Universitas ZXC. 6(2), 411–422. https://doi.org/10.52362/jisamar.v6i2.781

Wicaksono, W. W. (2022). Pengaruh Literasi Keuangan, Pengetahuan Investasi Dan Technology Acceptance Model (TAM) Terhadap Niat Masyarakat Blitar Berinvestasi di Pasar Modal.