JURNAL MEDIA AKADEMIK (JMA)
Vol.3, No.12 Desember 2025
e-ISSN: 3031-5220; DOI: 10.62281, Hal XX-XX
PT. Media Akademik Publisher
AHU-084213.AH.01.30.Tahun 2023

KESIAPAN ORGANISASI PENDIDIKAN TERHADAP RISIKO TEKNOLOGI DAN KEAMANAN DATA

Oleh:

Septia[1]

Universitas Negeri Padang
Alamat: JL. Prof. Dr. Hamka, Air Tawar Bar., Kec. Padang Utara, Kota Padang, Sumatera Barat (25171).
Korespondensi Penulis: septiatia554@gmail.com

Abstract. *The rapid digital transformation in educational institutions has significantly increased dependence on information technology for data management, administrative processes, and online learning systems. While digitalization improves efficiency and service quality, it also introduces substantial risks related to technology and data security that may disrupt educational operations. This study aims to analyze the organizational readiness of educational institutions in addressing technology risks and data security challenges. A qualitative approach was employed using a literature review method by examining relevant academic journals, reports, and international standards related to cybersecurity and information technology risk management in the education sector. The findings reveal that cyber threats such as malware, phishing, ransomware, data breaches, and insider threats can lead to disruptions in learning activities, financial losses, leakage of sensitive data, legal consequences, and reputational damage. These risks are further intensified by low cybersecurity awareness, weak technological infrastructure, inadequate information security governance, and the absence of comprehensive risk management practices. Therefore, this study highlights the importance of implementing information technology risk management, adopting security standards such as ISO/IEC 27001 and the Information Security Index (KAMI), and fostering a culture of security awareness through continuous training. An integrated strategy encompassing policy, technology, and human resources is essential to enhance digital resilience and safeguard information assets in educational institutions.*

Received November 25, 2025; Revised December 09, 2025; December 23, 2025
*Corresponding author: *septiatia554@gmail.com*

KESIAPAN ORGANISASI PENDIDIKAN TERHADAP RISIKO TEKNOLOGI DAN KEAMANAN DATA

Keywords: *Cybersecurity; Data Security; Educational Institutions; Information Technology Risk Management; Organizational Readiness*

Abstrak. Transformasi digital dalam institusi pendidikan telah meningkatkan ketergantungan pada teknologi informasi, termasuk dalam manajemen data, administrasi, dan proses pembelajaran daring. Namun, perkembangan ini juga memunculkan risiko signifikan terkait keamanan data dan ancaman siber yang mampu mengganggu operasional pendidikan secara menyeluruh. Studi ini menggunakan pendekatan kualitatif dengan metode studi literatur untuk menganalisis tingkat kesiapan organisasi pendidikan dalam menghadapi risiko teknologi dan keamanan data. Temuan penelitian menunjukkan bahwa ancaman siber seperti malware, phishing, ransomware, serta ancaman dari dalam organisasi dapat menyebabkan gangguan pembelajaran, kerugian finansial, pencurian data sensitif, hingga penurunan reputasi lembaga. Selain itu, kurangnya literasi keamanan, lemahnya infrastruktur, dan minimnya tata kelola risiko TI memperparah kerentanan institusi pendidikan. Penelitian ini menegaskan pentingnya penerapan manajemen risiko TI, standar keamanan seperti ISO 27001 dan KAMI, serta pembangunan budaya keamanan melalui pelatihan kepada seluruh warga satuan pendidikan. Dengan pendekatan strategis yang mengintegrasikan aspek kebijakan, teknologi, dan sumber daya manusia, institusi pendidikan dapat meningkatkan ketahanan digital dan melindungi aset informasinya secara lebih efektif.

Kata Kunci: Keamanan Siber; Keamanan Data; Institusi Pendidikan; Manajemen Risiko Teknologi Informasi; Kesiapan Organisasi

LATAR BELAKANG

Di tengah gelombang digitalisasi yang kian masif, institusi pendidikan, dari tingkat dasar hingga perguruan tinggi, telah bertransformasi menjadi lingkungan yang sangat berantung pada Teknologi Informasi (TI). Ketergantungan ini, yang mencakup manajemen data, administrasi, dan penyelenggaraan pembelajaran daring, bertujuan untuk meningkatkan efisiensi dan kualitas layanan pendidikan. Namun, transformasi digital ini, sebagaimana diungkapkan oleh Yusra Fadhillah et al. (2024), secara inheren membawa serta peningkatan dalam risiko teknologi dan keamanan data yang berpotensi serius mengganggu operasional dan merusak kredibilitas lembaga.

Risiko utama yang dihadapi oleh sektor pendidikan adalah ancaman siber yang semakin kompleks. Organisasi pendidikan sering dianggap sebagai sasaran yang relatif mudah karena infrastruktur keamanan yang lemah dan aset data yang sensitif. Silvia Paramita et al. (2022) menyoroti pentingnya pengamanan data operasional, seperti data siswa dan inventaris, yang krusial bagi kelancaran sistem informasi sekolah. Jika data ini terganggu, integritas akademik dan operasional seluruh lembaga dapat terancam, yang menuntut kesadaran kritis terhadap pentingnya keamanan data.

Tantangan dalam mencapai kesiapan siber tidak hanya bersifat teknis, tetapi juga organisasional dan sumber daya manusia. Reno Andre Permana et al. (2025) mengidentifikasi bahwa hambatan utama meliputi kurangnya penilaian risiko yang memadai, keterbatasan dalam adopsi alat keamanan yang canggih, dan tingkat kesadaran pengguna yang masih rendah terhadap ancaman siber. Kerentanan ini menunjukkan bahwa upaya penguatan keamanan harus melampaui sekadar investasi teknologi dan menyentuh aspek tata kelola serta budaya organisasi. Untuk mengatasi kesenjangan ini, diperlukan pendekatan strategis yang fokus pada Manajemen Risiko TI.

Menurut Yusra Fadhillah et al. (2024), pelatihan mengenai manajemen risiko TI sangat vital untuk melatih manajemen dan karyawan dalam mengidentifikasi, menganalisis, dan memitigasi risiko, yang pada akhirnya akan meningkatkan keamanan dan efisiensi operasional. Manajemen risiko yang terstruktur menjadi fondasi agar institusi dapat merespons ancaman secara proaktif, bukan hanya reaktif.

Selain manajemen risiko, standarisasi dan evaluasi kematangan keamanan juga menjadi komponen esensial. Silvia Paramita et al. (2022) menekankan pentingnya melakukan Analisis Manajemen Risiko Keamanan Data menggunakan kerangka kerja terstandardisasi, seperti yang mengacu pada Indeks Keamanan Informasi (KAMI) dan ISO 27001:2013. Penggunaan standar internasional ini memastikan bahwa kontrol keamanan yang diterapkan memiliki tingkat kematangan yang memadai dan kredibel, serta membantu mengidentifikasi area yang memerlukan perbaikan.

Secara paralel, adopsi metode dan teknologi perlindungan data yang mutakhir menjadi keharusan. Reno Andre Permana et al. (2025) menganalisis berbagai teknologi terbaru, termasuk peran Kecerdasan Buatan (AI) dalam deteksi ancaman dan otomatisasi keamanan, sebagai upaya untuk memperkuat pertahanan digital. Kesiapan organisasi pendidikan harus mencakup kemampuan untuk mengintegrasikan solusi-solusi canggih

ini untuk menciptakan lapisan perlindungan yang tangguh terhadap serangan yang terus berevolusi.

Dengan demikian, kesiapan organisasi pendidikan terhadap risiko teknologi dan keamanan data merupakan isu strategis yang multidimensi. Hal ini menuntut sinergi antara penerapan tata kelola Manajemen Risiko TI yang kuat, kepatuhan terhadap standar keamanan global, investasi dalam teknologi perlindungan data yang inovatif, dan yang paling penting, pengembangan kapasitas dan kesadaran Sumber Daya Manusia. Upaya komprehensif ini adalah kunci untuk memastikan keberlanjutan operasional, melindungi aset informasi yang sensitif, dan menjaga kepercayaan publik di era digital.

METODE PENELITIAN

Penelitian ini mengadopsi pendekatan Kualitatif Murni dengan jenis penelitian *Studi Literatur* (Literature Review). Metode ini dipilih karena tujuannya adalah membangun kerangka konseptual yang mendalam mengenai kesiapan organisasi pendidikan. Metode ini memungkinkan Sintesis Teoritis untuk memahami hubungan kompleks antara teori-teori manajer dan penerapannya dalam menghadapi isu teknologi dan keamanan data.

Pengumpulan data dengan menelusuri jurnal, buku, laporan, dan standar terkait risiko teknologi dan keamanan data di pendidikan melalui basis data ilmiah dan perpustakaan digital. Sedangkan analisis data dengan mengidentifikasi tema utama, mengkodekan informasi relevan, dan mensintesis temuan dari berbagai sumber literatur.

HASIL DAN PEMBAHASAN

Kejahatan siber atau cybercrime, secara sempit merefer kepada kejahatan yang berarsitektur pada sistem tertentu (Ambika & Senthilvel, 2020; Broadhurst et al., 2014; Dm et al., 2022; Maimon & Louderback, 2019; Suharto & Maria Novita Apriyani, 2021; Timofeyev & Dremova, 2022). Sedangkan secara luas cybercrime merupakan segala kejahatan baru yang meneriakan sasaran pada komputer atau jaringan komputer dan pengguna arus informan tersebut. Kejahatan cybercrime juga mencakup kejahatan konvensional yang melibatkan teknologi informasi dan komputer dan disebut sebagai kejahatan terkait komputer. Oleh karena itu, kejahatan cybercrime mencakup setiap kegiatan ilegal yang berkaitan dengan penggunaan komputer atau jaringan komputer, atau

yang berkaitan dengan jaringan komputer, atau yang dilakukan terhadap jaringan komputer.

Menurut Hapsari (2018), Cybercrime dapat didefinisikan sebagai kejahatan yang berkaitan dengan kepentingan pribadi atau kelompok tertentu. Banyak orang, baik secara langsung maupun tidak langsung, menggunakan teknologi untuk memperluas jangkauan kejahatan cybercrime. Seringkali, berbagai kepentingan, termasuk agama, politik, ekonomi, dan budaya, menunjukkan, mendorong, atau bahkan membenarkan seseorang atau sekelompok individu sebagai pelaku kejahatan siber. Motivasi ini menciptakan lingkungan dimana kejahatan dapat terjadi dengan mengembangkan sistem informasi dan komunikasi yang sudah ada (Hapsari & Pambayun, 2023).

Cybercrime maya adalah kejahatan yang terjadi ketika ada komunitas di dunia maya, khususnya di internet, dan memiliki karakteristik khusus yang membedakannya dari kejahatan biasa. Pertama, jenis kejahatan ini dilakukan di dunia maya, tempat tindakan ilegal, tidak sah, atau tidak bermoral terjadi, sehingga sulit untuk menentukan yurisdiksi yang tepat. Kedua, tindakan kriminal ini dilakukan melalui perangkat yang terhubung ke internet. Ketiga, jenis kerugian yang biasanya ditimbulkannya biasanya lebih besar, baik secara nyata maupun tidak nyata, termasuk, tetapi tidak terbatas pada, waktu, nilai, layanan, uang, barang, harga diri, martabat, informasi pribadi, dan banyak lagi. Selain itu, pelaku kriminal jenis ini biasanya mahir menggunakan internet dan aplikasinya. terakhir, kejahatan semacam ini biasanya melibatkan beberapa negara, melintasi batas negara, membuat penegakkan hukum lebih sulit. (Amin Suhaemin, 2023).

Serangan Siber yang Mengganggu Operasional Pendidikan

Konsekuensi Serangan Siber pada Institusi Pendidikan di antaranya yaitu:

1. Gangguan pada Proses Pembelajaran

Serangan siber dapat mengakibatkan gangguan besar pada proses pembelajaran. Jika sistem e-learning atau portal akademik terganggu, siswa tidak dapat mengakses materi pelajaran, mengumpulkan tugas, atau mengikuti ujian. Ini dapat menyebabkan penundaan dalam kalender akademik dan mempengaruhi hasil belajar siswa.

2. Kerugian Finansial

Biaya yang dikeluarkan untuk memulihkan sistem setelah serangan siber bisa sangat tinggi. Ini termasuk biaya forensik digital, penggantian perangkat keras/lunak yang

rusak, dan peningkatan keamanan. Selain itu, jika serangan tersebut melibatkan pencurian data keuangan, institusi mungkin juga harus menanggung kerugian akibat penipuan atau tuntutan hukum dari pihak yang terdampak

3. Penurunan Reputasi

Reputasi sebuah institusi pendidikan dapat terganggu jika mereka dianggap tidak mampu melindungi data dan sistem mereka dengan baik. Kepercayaan dari siswa orang tua, dan masyarakat dapat menurun, yang pada gilirannya dapat mempengaruhi pendaftaran siswa dan dukungan dari pemangku kepentingan lainnya.

4. Konsekuensi Hukum dan Kepatuhan

Institusi pendidikan menyimpan data pribadi dan sensitif (seperti data nilai, medis, dan keuangan) yang diatur oleh berbagai undang-undang privasi data (misalnya, GDPR di Eropa atau peraturan perlindungan data lokal). Serangan siber yang mengakibatkan kebocoran data dapat memicu sanksi hukum, denda yang besar, dan kewajiban notifikasi kepada pihak yang datanya dicuri. Kegagalan mematuhi regulasi ini dapat menambah beban finansial dan merusak citra institusi.

5. Pencurian Data Sensitif

Institusi pendidikan adalah target yang menarik karena mereka menyimpan sejumlah besar data pribadi yang kaya (Pendidikan, Keuangan, Kesehatan) dari siswa, staf, dan alumni. Serangan seperti ransomware atau pencurian basis data dapat menyebabkan data-data ini jatuh ke tangan pelaku kejahatan siber. Data ini kemudian dapat dijual di pasar gelap untuk tujuan pencurian identitas, penipuan akademik, atau serangan phishing yang ditargetkan.

Menurut Eduardus Taufan, seorang ahli keamanan siber dan pendiri *ISACA Indonesia Chapter*, institusi pendidikan sering menjadi target empuk karena memiliki anggaran keamanan siber yang terbatas dibandingkan sektor korporasi, sementara menyimpan data yang sama sensitifnya. "Institusi pendidikan harus sadar bahwa mereka bukan hanya tempat belajar, tetapi juga repositori data sensitif. Dampak serangan siber di sektor ini seringkali bersifat dua kali lipat: pertama, mengganggu fungsi vital mereka (proses belajar-mengajar); dan kedua, memicu konsekuensi hukum karena kelalaian dalam melindungi data pribadi, yang kini menjadi aset paling berharga bagi peretas. Investasi dalam awareness dan infrastruktur keamanan yang memadai adalah sebuah keharusan, bukan pilihan.

Kegunaan Menggunakan Keamanan Data

Kegunaan utama menerapkan pengamanan data ini tentu untuk melindungi data, baik itu data milik perusahaan dan konsumen. Selain itu, ternyata masih ada beberapa kegunaan lain yang bisa dirasakan dampak baiknya bagi pelaku usaha. Berikut adalah diantaranya.

1. Mencegah Serangan Siber, seperti yang sudah banyak disinggung di atas, pengamanan data digunakan untuk melindungi data dari serangan siber yang bisa mengganggu aktivitas operasional Perusahaan atau Organisasi pendidikan. Dengan menerapkan pengamanan yang benar, maka berbagai risiko bisa ditanggulangi dengan baik.
2. Melindungi Data, kegunaan paling utama dari pengamanan data ini data milik Perusahaan atau Organisasi Pendidikan maupun konsumen bisa terlindung dari serangan siber maupun jenis kejahatan lain. Dengan adanya keamanan data ini, maka berbagai ancaman serta risiko digital lainnya yang mengintai bisa diatasi ataupun dihindari dengan baik.
3. Menjaga Produktivitas Perusahaan, saat serangan siber menyerang, aktivitas operasional perusahaan biasanya juga ikut terganggu. Tapi jika perusahaan atau Organisasi Pendidikan sudah menerapkan pengamanan data dengan benar, maka risiko ini bisa ditangani dengan baik. Anda menjadi mengerti hal apa yang perlu dilakukan saat terjadi serangan siber, sehingga aktivitas perusahaan bisa tetap berjalan normal.

Di era digital saat ini, keamanan data telah menjadi perhatian utama bagi individu, organisasi, dan pemerintah di seluruh dunia. Data adalah aset yang sangat berharga, namun juga sangat rentan terhadap berbagai ancaman. Berikut ini adalah beberapa risiko keamanan data terbesar yang perlu diwaspadai dan dikelola dengan hati-hati.

1. Serangan Siber (Cyber Attacks), Serangan siber adalah ancaman utama dalam keamanan data, yang mencakup berbagai metode seperti malware, phishing, ransomware, dan Distributed Denial of Service (DDoS).
    a. Malware: Perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem komputer. Malware bisa dalam bentuk virus, worm, trojan, atau spyware.

b. Phishing: Teknik penipuan di mana penyerang mencoba untuk mendapatkan informasi sensitif seperti kata sandi dan nomor kartu kredit dengan menyamar sebagai entitas tepercaya melalui email atau pesan instan.
c. Ransomware: Jenis malware yang mengenkripsi data korban dan meminta tebusan untuk memulihkan akses. Contoh terkenal adalah serangan WannaCry yang melumpuhkan banyak organisasi di seluruh dunia.
d. DDoS: Serangan yang mencoba membuat layanan atau jaringan tidak dapat diakses dengan membanjiri target dengan lalu lintas internet yang berlebihan.

2. Kebocoran Data (Data Breaches)

Kebocoran data terjadi ketika data yang sensitif atau pribadi diakses dan diekspos oleh pihak yang tidak berwenang. Ini bisa disebabkan oleh serangan siber, kesalahan manusia, atau kegagalan sistem keamanan. Kesalahan konfigurasi misalnya, pengaturan cloud storage yang tidak aman dapat mengekspos data kepada publik. Kegagalan Sistem Keamanan seperti tidak menggunakan enkripsi yang kuat untuk data penting.

3. Ancaman Orang Dalam (Insider Threats)

Ancaman dari dalam organisasi, baik yang disengaja atau tidak disengaja, juga merupakan risiko besar. Orang dalam ini bisa saja karyawan, kontraktor, atau mitra bisnis yang memiliki akses ke sistem dan data.

a. Kesalahan Karyawan: Ketidaksengajaan seperti mengklik tautan berbahaya atau salah mengonfigurasi sistem.
b. Aksi Berbahaya oleh Karyawan: Misalnya, seorang karyawan yang berniat jahat mencuri data perusahaan untuk keuntungan pribadi atau untuk dijual kepada pihak ketiga.

4. Kelemahan pada Keamanan Sistem (System Vulnerabilities)

Banyak sistem informasi memiliki kelemahan yang bisa dieksploitasi oleh penyerang. Ini bisa termasuk software yang tidak terbarui, penggunaan kata sandi yang lemah, atau sistem yang tidak memiliki protokol keamanan yang tepat.

a. Software Tidak Terbarui: Pembaruan sistem dan patch sering kali dirilis untuk memperbaiki kerentanan. Sistem yang tidak terbarui rentan terhadap serangan yang memanfaatkan kelemahan ini.
b. Kata Sandi Lemah: Penggunaan kata sandi yang mudah ditebak atau tidak kompleks membuka peluang bagi penyerang untuk mengakses system

Strategi Menghadapi Risiko Teknologi dan Keamanan Data di Dunia Pendidikan

Pemanfaatan teknologi dalam proses belajar mengajar (transformasi digital) membawa risiko keamanan siber yang harus dikelola dengan bijak. Strategi yang komprehensif melibatkan aspek teknologi, kebijakan, dan sumber daya manusia (SDM).

1. Aspek Kebijakan dan Tata Kelola (Governance)

Strategi harus diawali dengan landasan kebijakan yang kuat untuk memastikan kepatuhan dan tata kelola yang baik. Penerapan kebijakan keamanan yang ketat, Institusi pendidikan harus menetapkan kebijakan tertulis mengenai penggunaan sistem TI, perlindungan data pribadi (siswa, staf, dan pengajar), serta prosedur tanggap insiden siber. Serta audit dan penilaian risiko berkala melakukan audit rutin terhadap infrastruktur TI untuk mengidentifikasi kerentanan dan menilai risiko yang ada (BSSN - 2024)

2. Aspek Teknologi (Technical Measures)

Penerapan teknologi keamanan yang andal adalah garis pertahanan utama dan memerlukan perencanaan yang matang. Penggunaan sistem keamanan lanjutan dan mengimplementasikan solusi keamanan seperti Firewall, Antivirus/Anti-Malware, dan jaringan secara real-time. Dimana pembaruan perangkat lunak dan sistem secara rutin untuk memastikan bahwa semua sistem operasi, aplikasi, dan perangkat lunak selalu diperbarui (patching) untuk mengatasi kerentanan keamanan yang telah diketahui (Resa Ramadani, UTI-TTIS). Anang Siswanto menekankan perlunya sikap kehati-hatian dan kewaspadaan yang harus diimbangi dengan investasi teknologi yang memadai bagi institusi pendidikan yang melakukan transformasi digital, mengingat risiko serangan siber yang terus berkembang.

3. Aspek Sumber Daya Manusia (Human Factors)

Faktor manusia sering menjadi titik lemah (weakest link), sehingga edukasi dan peningkatan kesadaran sangat penting. Pelatihan keamanan siber yang komprehensif dengan menyediakan pelatihan keamanan siber wajib untuk seluruh staf, pengajar, dan siswa. Materi meliputi cara mengenali Phishing dan Social Engineering, serta pentingnya kata sandi yang kuat. Peningkatan literasi digital dan kesadaran yang mendidik seluruh warga sekolah/universitas tentang pentingnya menjaga privasi data pribadi di dunia maya.

KESIMPULAN DAN SARAN

Bahwa kesiapan organisasi pendidikan dalam menghadapi risiko teknologi dan keamanan data masih menghadapi banyak tantangan. Serangan siber seperti malware, ransomware, phishing, serta kebocoran data terbukti mampu mengganggu proses pembelajaran, memicu kerugian finansial, memengaruhi reputasi, hingga mengakibatkan masalah hukum akibat pelanggaran perlindungan data pribadi. Kerentanan ini diperparah oleh lemahnya tata kelola keamanan informasi, kurangnya assessment risiko, serta keterbatasan institusi dalam mengadopsi teknologi perlindungan data yang memadai.

Kondisi tersebut menunjukkan bahwa ancaman siber bukan hanya persoalan teknis, tetapi juga menyangkut kesiapan manajerial dan budaya organisasi. Untuk meningkatkan ketahanan digital, institusi pendidikan perlu menerapkan manajemen risiko TI secara komprehensif, termasuk penyusunan kebijakan keamanan, audit berkala, dan kepatuhan terhadap standar internasional seperti ISO 27001:2013 dan Indeks KAMI. Di samping itu, investasi teknologi seperti firewall, IDS/IPS, sistem anti malware, serta pembaruan perangkat secara rutin menjadi keharusan.

Aspek sumber daya manusia merupakan elemen yang tidak dapat diabaikan, mengingat banyak insiden keamanan terjadi akibat human error. Oleh karena itu, pelatihan keamanan siber, peningkatan literasi digital, serta pembentukan budaya sadar keamanan menjadi langkah strategis untuk memastikan bahwa seluruh komponen dalam organisasi pendidikan mampu merespons ancaman siber secara proaktif dan efektif.

DAFTAR REFERENSI

Ambika, T., & Senthilvel, K. (2020). Cyber Crimes against the State: A Study on Cyber

Amin Suhaemin, M. (2023). Karakteristik Cybercrime Di Indonesia. *Journal of Islamic Law and Yurisprudance, Volume 5, Nomor 2* (2023) Pages 15–26.

Anggraeny, I., Monique, C., Puspitasari Wardoyo, Y., & Bhirini Slamet, A. (2022). The

Arifin, F. R. (2019). Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara (Cybercrime) Dalam Perkara Pencemaran Nama Baik Di Indonesia. Resman *Jurnal Hukum, Volume 5, Nomor 1, April 2019*, Hlm. 21-39 .

Fadhillah, Y., Siregar, M. N. H., Batubara, H. D. A., Aswan, N., & Hasibuan, F. A. (2024). Pelatihan Manajemen Resiko Teknologi Informasi Untuk Meningkatkan Keamanan dan Efisiensi Operasional di Lembaga Pendidikan. *JURNAL PENGABDIAN SOSIAL, 1(7),* Hal 518.

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime Di Indonesia: Sebuah *Jurnal Konstituen, 5(1), 1–17*. https://doi.org/10.33701/jk.v5i1.3208

Paramita, S., Siregar, S. A., Damanik, R. A., & Irawan, M. D. (2022). Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013. BULLETIN OF INFORMATION TECHNOLOGY (BIT), 3(4), 374–379.

Permana, R. A., Anindita, R., Zainol, Z., & Quinn, A. (2025). Analisis Metode dan Teknologi untuk Perlindungan Data dan Informasi dari Ancaman Siber. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi, 3(2), 137–146. Terrorism in India. Webology, 17(2).* https://doi.org/10.14704/WEB/V17I2/WEB17016