(2024), 2 (2): 139–151 Scientica 3021-8209
Jurnal Ilmiah Sain dan Teknologi

ANALISIS MANAJEMEN RISIKO BERBASIS ISO 27001 PADA ASPEK KEAMANAN SISTEM INFORMASI PADA PERUSAHAAN TOKOPEDIA

Derliana[1], Yulhendri[2]
Jurusan Sistem Informasi
Universitas Esa Unggul
Jalan Arjuna Utara No 9, Kebon Jeruk, Jakarta – 11510
E-mail : dderliana7@gmail.com, yulhendri@esaunggul.ac.id

Abstract (English)
Electronic data security is very important in information technology (IT) service providers and other industries, such as export and import companies, transportation, financial institutions, education, news, and banking that use IT facilities and place them as critical infrastructure. Information or data is an asset for the company. Data security can indirectly ensure business continuity, reduce risk, optimize return on investment and find business opportunities.In an increasingly advanced digital era, companies like Tokopedia are becoming increasingly dependent on sophisticated and integrated information systems. Information systems play a key role in company operations, customer data processing, and business transactions. However, as technology advances, information security risks are increasing. Threats such as cyberattacks, hacking, data leaks, and service disruptions can result in serious impacts on the company, including financial losses and reputational damage. To address these risks, ISO 27001-based risk management has become a widely recognized international reference. This standard provides comprehensive guidance and frameworks for managing information system security. with technological developments and evolving security threats.

Article History
Submitted: 7 January 2024
Accepted: 16 January 2024
Published: 17 January 2024

Key Words
ISO 27001, Tokopedia, Risk Management.

Abstrak (Indonesia)
Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa teknologi informasi (TI) maupun industri lainnya, seperti perusahaan export import, tranportasi, lembaga keuangan, pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting). Informasi atau data adalah aset bagi perusahaan. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan return on investment dan mencari kesempatan bisnis.Dalam era digital yang semakin maju, perusahaan seperti Tokopedia menjadi semakin bergantung pada sistem informasi yang canggih dan terintegrasi. Sistem informasi memainkan peran kunci dalam operasional perusahaan, pengolahan data pelanggan, dan transaksi bisnis. Namun, seiring dengan kemajuan teknologi, risiko keamanan informasi semakin meningkat. Ancaman seperti serangan siber, peretasan, kebocoran data, dan gangguan layanan dapat mengakibatkan dampak serius pada perusahaan, termasuk kerugian finansial dan kerusakan reputasi. Untuk mengatasi risiko ini, manajemen risiko berbasis ISO 27001 telah menjadi acuan internasional yang diakui secara luas. Standar ini memberikan panduan dan kerangka kerja yang komprehensif untuk mengelola keamanan sistem informasi. dengan perkembangan teknologi dan ancaman keamanan yang terus berkembang.

Sejarah Artikel
Submitted: 7 January 2024
Accepted: 16 January 2024
Published: 17 January 2024

Kata Kunci
ISO 27001, Tokopedia, Manajemen Risiko

Pendahuluan

Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa teknologi informasi (TI) maupun industri lainnya, seperti perusahaan export import, tranportasi, lembaga keuangan, pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting). Informasi atau data adalah aset bagi perusahaan. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan return on investment dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan disharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan. Untuk menciptakan lingkungan yang aman, organisasi perlu mewaspadai ancaman yang dapat menyerang baik dari luar maupun dari dalam. Kemampuan mengantisipasi berbagai ancaman informasi harus didasarkan pada tiga prinsip, yaitu kerahasiaan, integritas, dan ketersediaan informasi Dengan menerapkan ketiga prinsip tersebut, perusahaan dapat menciptakan keamanan informasi sesuai ISO 27001.

Dalam era digital yang semakin maju, perusahaan seperti Tokopedia menjadi semakin bergantung pada sistem informasi yang canggih dan terintegrasi. Sistem informasi memainkan peran kunci dalam operasional perusahaan, pengolahan data pelanggan, dan transaksi bisnis. Namun, seiring dengan kemajuan teknologi, risiko keamanan informasi semakin meningkat. Ancaman seperti serangan siber, peretasan, kebocoran data, dan gangguan layanan dapat mengakibatkan dampak serius pada perusahaan, termasuk kerugian finansial dan kerusakan reputasi. Untuk mengatasi risiko ini, manajemen risiko berbasis ISO 27001 telah menjadi acuan internasional yang diakui secara luas. Standar ini memberikan panduan dan kerangka kerja yang komprehensif untuk mengelola keamanan sistem informasi. dengan perkembangan teknologi dan ancaman keamanan yang terus berkembang.

Tokopedia juga menjalin kerjasama dengan lembaga dan organisasi yang terkait dengan keamanan informasi seperti CERT (Computer Emergency Response Team) untuk meningkatkan respons terhadap serangan keamanan. Tokopedia juga berkomitmen untuk mematuhi standar keamanan informasi yang telah ditetapkan oleh pemerintah Indonesia dan lembaga internasional lainnya seperti ISO 27001. Dengan mengadopsi teknologi terkini, melibatkan sumber daya manusia yang terampil, dan menjalin kerjasama dengan lembaga terkait, Tokopedia berusaha memastikan keamanan sistem informasi perusahaannya. Namun demikian, upaya tersebut harus terus ditingkatkan dan disesuaikan dengan perkembangan teknologi dan ancaman keamanan yang terus berkembang. Oleh karena itu, Tokopedia selalu melakukan evaluasi terhadap sistem keamanan informasinya guna memastikan keamanan dan privasi pengguna tetap terjaga.

Tinjauan Pustaka

a. Analisi Risiko

Analisis risiko adalah aktivitas menentukan tingkat kemungkinan atau frekuensi suatu risiko dan tingkat dampak dari suatu risiko dengan memperhatikan penanganan risiko yang sudah dilakukan, dan diakhiri dengan menentukan tingkatan dari risiko. Analisis risiko dilakukan dengan beberapa tahapan sebgai berikut :

- Unit pemilik risiko memberikan skor kemungkinan atau frekuensi dan skor dampak untuk setiap risiko yang telah teriidentifikasi. Pemberian skor dilakukan mengacu pada

kriteria kemungkinan/frekuensi dan kriteria damoak yang sudah ditentukan pada tahap penentuan konteks dengan memperhatikan penanganan risiko yang selama ini sudah dilakukan.
- Unit Pemilik Risiko menghitung tingkat risiko untuk masingmasing risiko dengan cara mengalikan skor tingkat kemungkinan/frekuensi dengan skor tingkat dampak untuk setiap risiko.

b. Keamanan Informasi

Keamanan informasi berkaitan dengan melindungi aset informasi terhadap kehilangan atau kerusakan data yang menjamin kelangsungan bisnis dan meminimalkan risko bisnis. keamanna informasi dapat dicapai dengan beberapa strategi sesuai dengan kebutuhan dan keamanan informasi memiliki beberapa aspek diantaranya adalah:

- Confidentiality (kerahasiaan)
  Segala aspek dari informasi yang bersifat rahasia dari pengguna yang tidak berkepentingan dan hanya orang tertentu atau orang yang berwenang saja yang bisa mengakses informasi tersebut.
- Integrity (integritas)
  Keamanan yang menjamin aset tersebut tidak melakukan perubahan atau modifikasi terhadap proses dan penyimpanan informasi dari pihak berwewenang untuk Menjaga keakuratan, serta kelengkapan data dari ancaman pihak luar yang tidak berkepentingan.
- Avability (ketersediaan)
  Menjamin bahwa data dan informasi yang ada pada saat diperlukan oleh pihak berwenang dan memastikan bahwa informasi tersedia dan mudah di akses tanpa adanya gangguan dari pihak luar. Selain data dan informasi, mekanisme authentication, saluran akses dan sistem operasi nya harus berfungsi dengan baik agar data terlindungi dan memastikan data tersedia saat dibutuhkan.

c. Manajemen Risiko

Manajemenn risiko merupakan usaha yang dilakukan untuk memperhitungkan segala dampak negatif dan menerapkan prosedur agar dapat meminimalisir risiko yang terjadi dengan cara mengidentifikasi risiko, menganalisa risiko, dan melakukan penanganan untuk mengurangi risiko sampai dampaknya terhadap proses bisnis di organisasi pada level diperbolehkan. Tujuan dari manajemen risiko untuk mengurangi atau meminimalkan adanya kemungkinan kegagalan yaitu dengan cara dihadapi dan dimitigasi terhadap teknologi informasi tersebut.

d. ISO 27001

ISO (International Organization for Standardization) adalah sistem khusus untuk standarisasi di seluruh dunia yang didalamnya berisi tentang spesifikasi atau persyaratan yang harus dipenuhi dalam membangun dan pengelolaan keamanan informasi melalui Sistem Manajemen Keamanann Informasi (SMKI). ISO 27001 merupakan standar internasional untuk untuk melakukan pendekatan pada manajemen risiko, memastikan otoritas terkait bahwa risiko telah dikelola dengan baik, untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi.

Hasil dan Pembahasan

a. Analisis keamanan informasi

Pada analisis keamanan informasi tim peneliti harus memahami proses bisnis dan IT yang ada di PT. Tokopedia. Pemahaman yang harus dipelajari oleh tim peneliti adalah mempelajari dokumen yang berhubungan dengan data PT Tokopedia yaitu profil perusahaan, visi dan misis perusahaan, struktur organisasi perusahaan, serta proses dan bisnis IT perusahaan, tim peneliti harus mengetahui apakah perusahaan sudah melakukan keamanan sistem informasi berdasarkan iso 27001.

b. Analisis Business Context

Berdasarkan analisis data isu ekstrenal dan internal maka didapatkan ruang lingkup sistem keamanan Informasi di tokopedia:

- Sistem
- Data
- People

c. Indetifikasi Aset

Dalam mengedintifikasi aset perusahaan dibagi dalam tiga jenis yaitu pertama aset sistem dan aplikasi yang dibutuhkan atau yang digunakan perusahaan, kedua aset Data yang ada dalam perusahaan dan yang ketiga aset manusia (people) yaitu orang – orang yang memiliki keterampilan atau pengetahuan khusus dan penting bagi perusahaan. berikut adalah hasil dari identifikasi aset perusahaan tokopedia.

Data Aset

Kategori	Aset
Hardware	Server
	Akses Poin
	Router
	Kabel
	RFID
	Kamera CCTV
	Smart TV
	PC, Keyboard dan Mouse
	Camtouch
	Harddisk dan Flashdisk
Software	Aplikasi tokopedia
	Promox virtual Envoirement
	Server Backup tokopedia
	Database tokopedia
Data / Informasi	Data identitas pelanggan
	Data produk
	Data pemesanan
	Data transaksi
	Data logistik

	Data identitas pegawai
	Data Infrastruktur
	Data Keuangan
People / Sumber daya manusia	Direktur
	HRD
	Karyawan
	Staff
	Pelanggan

d. Analisis Risiko

Setelah data aset didapatkan selanjutnya melakukan analisis risiko pada masing – masing aset yang sudah diidentifikasi seperti gambar dibawah ini:

Kategori	Aset	Threat	Vulnerability	Risiko
Hardware	Server	Kebakaran dan bencana alam	Masih kurangnya alat pendektesi untuk kebakaran dan penanganan yang baik saat terjadi bencana alam dan kebakaran	Perangkat rusak yang dapat memnyebabkan data yang disimpan akan hilang, sehingga server tidak berfungsi dengan baik dan tidak dapat di akses.
	Kabel	Kebakaran dan bencana alam	Masih kurangnya alat pendektesi untuk kebakaran dan penanganan yang baik saat terjadi bencana alam dan kebakaran	Menyebabkan kabel terkelupas atau sampai putus yang mengakibatkan seluruh komponen yang menggunakan kabel tidak dapat berfungsi
Software	Aplikasi Tokopedia	Aplikasi down	Server mengalami peningkatan trafik	Aplikasi dan informasi tidak dapat di akses
		Aplikasi terjadi bug	Terjadi masalah pada bagian dalam penulisan kode	Sistem tidak dapat di akses, dijalanlan dengan semestinya, dan beresiko diretas oleh pihak yang tidak bertanggung jawab
Data / Informasi	Data identitas pelanggan	Kehilangan data	Kurangnya pada back up data dan tidak melakukan back up data setiap saat.	Data/informasi tidak dapat dibuka atau data yang disimpan akan hilang

	Data identitas pegawai	Pencurian data	Kurangnya keamanan informasi dan penyalah gunaan akses	Bocornya data penting perusahaan kepada pihak yang tidak bertanggung jawab yang nanti nya akan di salah gunakan, data yang ada sudah tidak valid karena sudah di ubah atau di ganti data nya
People / SDM	Pelanggan	Password tidak sesuai atau salah	Password yang dimasukan tidak sesuai	Lupa password atau data tidak valid karena sudah di ubah atau sudah dihapus oleh pihak yang tidak bertanggung jawab

e. Pengelolaan Risiko

Setelah risiko diidentifikasi selanjutnya yaitu diidentifikasi nilai kemungkinan dan dampak dengan menggunakan matriks 5x5.

kemungkinan	**Dampak /Akibat**				
	1	2	3	4	5
1	Sangat rendah	Sangat rendah	Sangat rendah	Sangat rendah	Sangat rendah
2	Sangat rendah	Sangat rendah	Rendah	rendah	rendah
3	Sangat rendah	Rendah	Rendah	Moderat	Moderat
4	Sangat rendah	Rendah	Moderat	Tinggi	Sangat tinggi
5	Sangat rendah	Rendah	Moderat	Sangat tinggi	Sangat tinggi

f. Penentuan Level Risiko

Dalam analisis risiko yaitu melakukan penilaian risiko dengan memasukan kategori dampak dan kemungkinan dengan range nilai 1-5.

Hasil penentuan Level Risiko

Aset	Risiko	Dampak	Likelihood	Matrik Score	Risk Level
Server	Perangkat rusak yang dapat menyebabkan data yang disimpan akan hilang, sehingga server tidak berfungsi	5	5	25	H

	dengan baik dan tidak dapat di akses.				
Kabel	Menyebabkan kabel terkelupas atau sampai putus yang mengakibatkan seluruh komponen yang menggunakan kabel tidak dapat berfungsi.	5	5	25	H
Aplikasi Tokopedia	Aplikasi dan informasi tidak dapat di akses	5	4	20	H
	Sistem tidak dapat di akses, dijalanlan dengan semestinya, dan beresiko diretas oleh pihak yang tidak bertanggung jawab	4	5	20	H
Data identitas pelanggan	Data/informasi tidak dapat dibuka atau diakses	4	5	20	H
Data identitas pegawai	Bocornya data penting perusahaan kepada pihak yang tidak bertanggung jawab yang nanti nya akan di salah gunakan, data yang ada sudah tidak valid karena sudah di ubah atau di ganti data nya	5	5	25	H
Pelanggan	Lupa password atau data tidak valid karena sudah di ubah atau sudah dihapus oleh pihak yang tidak bertanggung jawab	5	3	15	H

g. Penanganan Risiko

Penanganan risiko dilakukan untuk menentukan langkah penanganan risiko sesuai dengan kriteria – kriteria penangan risiko penangan risiko yaitu, risiko diterima (risk acceptance), risiko direduksi (risk reduction), risiko ditolak (risk avoidance) dan risiko dialihkan (risk transfer). Untuk penangana risiko dilihat dari level risiko tidak dapat diterima ketika level risikonya berada pada level high.

Penanganan Risiko

Aset	Risiko	Risk Level	Penangan Risiko
Server	Perangkat rusak yang dapat menyebabkan data yang disimpan akan hilang, sehingga server tidak berfungsi dengan baik dan tidak dapat di akses	H	Risk Avoidance
Kabel	Menyebabkan kabel terkelupas atau sampai putus yang mengakibatkan seluruh komponen yang menggunakan kabel tidak dapat berfungsi.	H	Risk Avoidance
Aplikasi Tokopedia	Aplikasi dan informasi tidak dapat di akses	H	Risk Avoidance
	Sistem tidak dapat di akses, dijalanlan dengan semestinya, dan beresiko diretas oleh pihak yang tidak bertanggung jawab		
Data identitas pelanggan	Data/informasi tidak dapat dibuka atau diakses	H	Risk Avoidance
Data identitas pegawai	Bocornya data penting perusahaan kepada pihak yang tidak bertanggung jawab yang nanti nya akan di salah gunakan, data yang ada sudah tidak valid karena sudah di ubah atau di ganti data nya	H	Risk Avoidance
Pelanggan	Lupa password atau data tidak valid karena sudah di ubah atau sudah dihapus oleh pihak yang tidak bertanggung jawab	H	Risk Avoidance

h. Kontrol Pengendalian Risiko

Kontrol pengendalian risiko diambil sesuai dengan ISO 27001

Domain ISO 27001

A.9.4	**System and application access control**
A.9.4.1	Information access restricition
A.9.4.2	Secure log-on procedures
A.9.4.3	Password management system
A.9.4.4	Use of privileged utility programs
A.9.4.5	Access control to program source code
A.11	**Physical and environmental security**
A.11.1	Secure areas
A.11.1.1	Physical security perimeter

A.11.1.2	Physical entry controls
A.11.1.3	Securing office, room and facilites
A.11.1.4	Protecting against external and environmental threats
A.11.1.5	Working in secure areas
A.11.1.6	Delivery and loading areas
A.12	**Operations Security**
A.12.1	Operational Procedures and Responsibilities
A.12.1.1	Documented operating procedures
A.12.1.2	Change management
A.12.1.3	Capacity management
A.12.1.4	Separation of development, test and operational environments
A.12.3	**Back-UP**
A.12.3.1	Information backup
A.16	**Information security incdent management**
A.16.1	Management of information security incidents and improvement

- **Kontrol Pengendalian Risiko**

Aset	Threat	Risiko	Penanganan	Kontrol Kemanan
Server	Kebakaran dan bencana Alam	Perangkat rusak yang dapat menyebabkan data yang disimpan akan hilang, sehingga server tidak berfungsi dengan baik dan tidak dapat di akses	Melakukan Backup data untuk berjaga jaga ketika data hilang atau tidak dapat di akses	A.11.1.4 Protecting against external and environmental threats
Kabel	Kebakaran Dan Bencana Alam	Menyebabkan kabel terkelupas atau sampai putus yang mengakibatkan seluruh komponen yang menggunakan kabel tidak dapat berfungsi.	Pilih lokasi pemasangan kabel yang tidak rentan terhadap bencana alam seperti banjir, tanah longsor, atau daerah rawan gempa bumi. Perhatikan topografi dan kondisi lingkungan sekitarnya sebelum memasang kabel	A.11.1.4 Protecting against external and environmental threats

Aplikasi Tokopedia	Aplikasi down	Aplikasi dan informasi tidak dapat di akses	Gunakan perangkat lunak monitoring server yang memungkinkan Anda untuk memantau kinerja server secara terus-menerus. Ini membantu dalam mendeteksi masalah sejak dini sebelum berpotensi menyebabkan kegagalan server.	A.12.1.3 Capacity management
	Aplikasi terjadi bug	Sistem tidak dapat di akses, dijalanlan dengan semestinya, dan beresiko diretas oleh pihak yang tidak bertanggung jawab	Gunakan praktik pengembangan perangkat lunak yang aman, seperti pemeriksaan kode, validasi input, penyaringan data, serta memastikan penggunaan API dan library yang aman.	A.12.1.3 Capacity management
Data identitas pelanggan	Kehilangan data	Data/informasi tidak dapat dibuka atau diakses	Melakukan Backup data untuk berjaga jaga ketika data hilang atau tidak dapat di akses	A.12.3.1 Information backup
Data identitas pegawai	Kebocoran data	Bocornya data penting perusahaan kepada pihak yang tidak bertanggung jawab yang nanti nya akan di salah gunakan, data yang ada sudah tidak valid karena sudah di ubah atau di ganti data nya	Enkripsi data sensitif, baik saat data berada dalam perjalanan (melalui protokol HTTPS atau VPN) maupun saat disimpan di server. Enkripsi mempersulit akses ilegal terhadap informasi penting.	A.16.1 Management of information security incidents and improvements

Pelanggan	Password tidak sesuai atau salah	Lupa password atau data tidak valid karena sudah di ubah atau sudah dihapus oleh pihak yang tidak bertanggung jawab	Gunakan aplikasi pengelola kata sandi yang aman dan terpercaya. Password manager dapat menyimpan semua kata sandi Anda dalam satu tempat yang terenkripsi dan memerlukan kata sandi utama untuk mengaksesnya. Mereka sering menyediakan fitur autentikasi dua faktor (2FA) untuk lapisan keamanan tambahan	A.9.4.3 Password management system

Daftar Pustaka

Alexei, A. (2021). Ensuring Information Security in Public Organizations in the Republic of Moldova Through the Iso 27001 Standard. *Journal of Social Sciences*, *IV(1)*. https://doi.org/10.52326/jss.utm.2021.4(1).11

Apriandari, W., & Sasongko, A. (2019). Daerah Kota Sukabumi (Studi Kasus: Di Diskominfo Kota Sukabumi). *Jurnal Ilmiah SANTIKA*, *8*(1), 715–729. www.tecnoid.id

Armadyana, R., Yasirandi, R., & Makky, M. Al. (2023). *Analisis dan Penilaian Risiko Keamanan Informasi Menggunakan OCTAVE Allegro (Studi Kasus : PT . XYZ)*. *10*(3), 3690–3703.

Clarissa, S., & Wang, G. (2023). *Keywords: information security; maturity level; ISO/IEC; ISO 27001:2013*. *4*(9), 1361–1371. https://doi.org/10.59141/jist.v4i9.739

Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, *1*(1), 1–11. https://doi.org/10.25008/bcsee.v1i1.2

Fitrani, L. D. (2022). Risk Risk Assessment and Development of Access Control Information Security Governance Based on ISO/IEC 27001:2013 At XYZ University. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *9*(2), 891–907. https://doi.org/10.35957/jatisi.v9i2.1643

Isnaini, K. N., & Suhartono, D. (2023). Security Analysis of Simpel Desa using Mobile Security Framework and ISO 27002:2013. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *7*(1), 84–105.

https://doi.org/10.29407/intensif.v7i1.18742

Kristanto, T., Sholik, M., Rahmawati, D., & Nasrullah, M. (2019). Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ. *JISA(Jurnal Informatika Dan Sains)*, *2*(2), 30–33. https://doi.org/10.31326/jisa.v2i2.497

Legowo, N., & Juhartoyo, Y. (2022). Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001. *Journal of System and Management Sciences*, *12*(3), 181–199. https://doi.org/10.33168/JSMS.2022.0310

Nurfadilah, D. R., Putra, W. N. H., & Rachmadi, A. (2020). Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001 : 2013 (Studi Kasus : Aplikasi E-Kinerja). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *Universitas Brawijaya*, *4*(9), 3014–3020.

Paramita, S., Siregar, S. A., Damanik, R. A., & ... (2022). Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001: 2013. *Bulletin of Information …*, *3*(4), 374–379. https://journal.fkpt.org/index.php/BIT/article/view/421%0Ahttps://journal.fkpt.org/index.php/BIT/article/download/421/263

Ridwan, A. (2020). *Analysis of Implementation of Information Security Based on ISO / IEC 27001 : 2013 (Case study at the Indonesian Insurance Company)*. *5*(2), 140–149.

Sholikhatin, S. A., & Isnaini, K. N. (2021). Analysis of Information Security Using ISO 27001 and Triangular Fuzzy Number Weighting. *Jurnal Ilmiah Informatika*, *6*(1), 43–49. https://doi.org/10.35316/jimi.v6i1.1224

Sholikhatin, S. A., Setyanto, A., & Luthfi, E. T. (2019). Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto). *Jurnal Ilmiah IT CIDA*, *4*(1), 1–9. https://doi.org/10.55635/jic.v4i1.75

Soesanto, E., Adrian, M. R., Syifaa, N., & Suwandi, A. (2023). *IJM : Indonesian Journal of Multidisciplinary Analisis Keamanan Sistem Informasi di PT . Telkom Menggunakan Indeks KAMI*. *1*, 169–175.

Sulistyowati, I., & Ginardi, R. V. H. (2019). Information Security Risk Management with Octave Method and ISO/EIC 27001: 2013 (Case Study: Airlangga University). *IPTEK Journal of Proceedings Series*, *0*(1), 32–38.

Tanaamah, A. R., & Indira, F. J. (2021). Analysis of Information Technology Security Management UKSW SIASAT Using ISO/IEC 27001:2013. *IJITEE (International Journal of Information Technology and Electrical Engineering)*, *5*(2), 68. https://doi.org/10.22146/ijitee.65670

Tuga, M. A., & Aziz, A. (2019). Analisis Manajemen Keamanan Sistem Informasi Akademik Universitas Kanjuruhan Malang Menggunakan Standar Iso 27001: 2013. *Semnas SENASTEK Unikama 2019*, *2*, 764–771. https://conference.unikama.ac.id/artikel/index.php/senastek/article/view/257

Tutik, Mutiah, N., & Rusi, I. (2022). ANALISIS DAN MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS (FMEA) DAN KONTROL ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Sambas). *CODING : Jurnal Komputer Dan Aplikasi*, *10*(02), 249–261. https://jurnal.untan.ac.id/index.php/jcskommipa/article/view/55082%0Ahttps://jurnal.untan.ac.id/index.php/jcskommipa/article/viewFile/55082/75676595021

Edy Soesanto, Alfonso Lande, Heru Tian Sanjaya, & Muhammad Rafli Hermawan. (2023). Analisis Sistem Manajemen Keamanan Di Perusahaan Tokopedia Dalam Menigkatkan Proteksi Data Dan Privasi Pengguna. *Jurnal Kewirausahaan Dan Manajemen Bisnis: Cuan*, *1*(1), 21–29. https://doi.org/10.59603/cuan.v1i1.14