Manajemen Risiko Keamanan Informasi Menggunakan Standar ISO 27001:2022 Studi Kasus Komisi Pemilihan Umum

Sabillah Sakti[1], Ferdhyan Wahyu Listyanto[2], Rachel Irda Damayanti[3]
Mastuty Ayu Ningtyas[4]
sabillahsakti@student.telkomuniversity.ac.id[1],
ferdhyan@student.telkomuniversity.ac.id[2],
rachelirda@student.telkomuniversity.ac.id[3]
mastutyayu@telkomuniversity.ac.id[4]

Abstrak

Perlindungan informasi menjadi sangat penting untuk menjaga keamanan suatu organisasi. Komisi Pemilihan Umum (KPU) mengumpulkan dan memproses informasi sensitif, sehingga memerlukan sistem manajemen risiko keamanan informasi yang efektif. Penelitian ini bertujuan untuk menganalisis penerapan standar ISO 27001:2022 dalam manajemen risiko keamanan informasi di KPU. Metode yang digunakan adalah Failure Mode and Effects Analys (FMEA), yang melibatkan analisis konteks bisnis, identifikasi aset, identifikasi risiko, dan pengelolaan risiko. Hasil penelitian menunjukkan bahwa terdapat 20 risiko yang mana 50% diantaranya memiliki level very high yang harus diperioritaskan untuk mencegah resiko itu terjadi.

Kata kunci: KPU, FMEA, ISO 27001:2022, ANALISIS RISIKO

Abstract

Information protection is very important to maintain the security of an organization. The General Election Commission (KPU) collects and processes sensitive information, thus requiring an effective information security risk management system. This study aims to analyze the application of the ISO 27001: 2022 standard in information security risk management at KPU. The method used is Failure Mode and Effects Analysys (FMEA), which involves business context analysis, asset identification, risk identification, and risk management. The results showed that there are 20 risks of which 50% have a very high level that must be prioritized to prevent the risk from occurring.

Key word: *KPU, FMEA, ISO 27001:2022, RISK ANALYSIS*

PENDAHULUAN

Dalam era digital yang semakin kompleks dan dinamis, perlindungan informasi menjadi salah satu aspek yang sangat penting dalam menjaga keamanan dan integritas organisasi. Informasi yang dikumpulkan dan diproses oleh organisasi dapat berupa data pribadi, transaksi keuangan, atau informasi strategis yang sangat sensitif. Oleh karena itu, manajemen risiko keamanan informasi menjadi sangat penting untuk mencegah dan mengurangi potensi

kerugian yang dapat disebabkan oleh serangan siber, kebocoran data, atau penggunaan informasi secara tidak sah(Nurillah and Trihandoyo 2024).

Standar ISO 27001:2022 adalah salah satu standar yang paling populer dan digunakan secara global dalam manajemen risiko keamanan informasi. Standar ini memberikan pedoman yang jelas dan spesifik untuk organisasi dalam mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi. Dengan menggunakan standar ini, organisasi dapat meningkatkan kemampuan dalam mengidentifikasi dan mengelola risiko keamanan informasi, serta meningkatkan keamanan dan integritas informasi(Kurniawan and Salman 2023).

Komisi Pemilihan Umum (KPU) adalah organisasi yang sangat penting dalam menjaga keamanan dan integritas informasi, terutama dalam proses pemilihan umum. KPU adalah lembaga pemerintah yang dibentuk berdasarkan Pasal 22E Undang-Undang Dasar 1945 pada amandemen ketiga. Lembaga ini bersifat nasional, tetap, dan mandiri(Fuad Amirullah, Syariful Alam, and M.Imam Sulistyo S 2023). KPU mengumpulkan dan memproses informasi yang sangat sensitif, seperti data pribadi pemilih, data hasil pemilihan, dan informasi strategis lainnya. Oleh karena itu, KPU harus memiliki sistem manajemen risiko keamanan informasi yang efektif untuk mencegah dan mengurangi potensi kerugian yang dapat disebabkan oleh serangan siber, kebocoran data, atau penggunaan informasi secara tidak sah. Dalam penelitian ini, KPU dipilih sebagai subjek studi untuk menganalisis bagaimana standar ISO 27001:2022 dapat diterapkan dalam manajemen risiko keamanan informasi.

Manajemen risiko keamanan sistem informasi di KPU sangat penting karena untuk pertama kalinya KPU menggunakan teknologi bernama Sirekap. Sirekap adalah aplikasi berbasis teknologi informasi yang digunakan untuk mempublikasikan hasil penghitungan suara dan rekapitulasi hasil penghitungan suara, serta sebagai alat bantu dalam proses rekapitulasi hasil penghitungan suara pada pemilihan(Gauru, Martini, and Alfirdaus 2022). Oleh karena itu, perlu dilakukan identifikasi risiko untuk menghindari potensi risiko yang mungkin terjadi.

Dengan demikian, penelitian ini bertujuan untuk menganalisis bagaimana standar ISO 27001:2022 dapat diterapkan dalam manajemen risiko keamanan informasi di KPU, serta mengetahui bagaimana KPU dapat meningkatkan keamanan informasi dengan menggunakan standar ini. Penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan teori dan praktik manajemen risiko keamanan informasi, serta memberikan referensi yang berguna bagi organisasi lain yang ingin meningkatkan keamanan informasi dengan menggunakan standar ISO 27001:2022.

TINJAUAN PUSTAKA

1. ISO 27001:2022

ISO 27001:2022 adalah standar internasional yang diterbitkan oleh International Organization for Standardization (ISO) yang mengatur sistem manajemen keamanan informasi (Information Security Management System/SMKI). Standar ini memberikan kerangka kerja yang komprehensif bagi organisasi dalam mengelola keamanan informasi dengan efektif. Standar

ini resmi dipublikasi pada bulan Oktober 2022, meskipun standar pendahulunya yaitu ISO 27001-2013 masih dapat digunakan selama masa transisi hingga Oktober 2025. ISO 27001:2022 berfokus pada perlindungan informasi penting bagi organisasi, termasuk data sensitif, informasi pelanggan, informasi keuangan, dan informasi lain yang bernilai penting. Standar ini dirancang untuk membantu organisasi dalam membangun, menerapkan, mengoperasikan, memantau, memelihara, dan meningkatkan sistem manajemen keamanan informasi mereka. Standar ini mencakup berbagai aspek keamanan informasi, termasuk kebijakan keamanan informasi, identifikasi aset informasi, analisis risiko, pengendalian keamanan informasi, manajemen insiden keamanan, dan tinjauan berkelanjutan(Sinaga 2024).

2. **Failure Mode and Effects Analysis**

   FMEA (Failure Mode and Effects Analysis) adalah cara terstruktur untuk mengidentifikasi dan mengatasi masalah potensial atau kegagalan pada sistem sebelum terjadi efek yang buruk. Tujuannya adalah untuk mencegah terjadinya masalah pada produk dan proses. Dengan menggunakan desain dan proses manufaktur, metode ini dapat mengurangi biaya dengan cara mengidentifikasi dan meningkatkan produk dan proses yang tidak membutuhkan banyak biaya dan mudah dilakukan(Hanifah and S Suroso 2020).

METODE

Dalam penelitian ini, metode yang digunakan adalah *Failure mode and effects analysis* (FMEA) sesuai dengan standar ISO 27001, yang melibatkan beberapa tahap, yaitu:

1. **Analisis konteks bisnis:** Meliputi analisis isu internal dan eksternal organisasi serta penentuan ruang lingkup perusahaan yang mana dalam penelitian ini adalah KPU.
2. **Identifikasi aset:** Aset diklasifikasikan menjadi empat kategori yaitu hardware, software, personel, dan data/informasi.
3. **Identifikasi risiko:** Mengidentifikasi risiko yang akan terjadi pada setiap aset.
4. **Pengelolaan risiko:** Melakukan penilaian risiko dengan rentang nilai 1 – 10 untuk setiap aset berdasarkan ancaman dan kerentanannya berdasarkan hasil observasi dan wawancara.

3.1 Tabel Acuan Penilaian Risiko

Severity (S)	Occurrence (O)	Detection (D)	Rating
Hazardous without warning	Very high failure is almost inevitable	Absolute uncertainty	10
Hazardous with warning	Very high failure is almost inevitable	Very remote	9

Severity (S)	Occurrence (O)	Detection (D)	Rating
Very high	High repeated failures	Remote	8
High	High repeated failures	Very low	7
Moderate	Moderate occasional failures	Low	6
Low	Moderate occasional failures	Moderate	5
Very low	Moderate occasional failures	Moderately high	4
Minor	Low relatively few failures	High	3
Very minor	Low relatively few failures	Very high	2
None	Remote failure is unlikely	Almost certain	1

5. **Penentuan *Risk Priority Number(*RPN)** dilakukan dengan mengalikan nilai *Severity, Occurence,* dan *Detection* dari masing-masing risiko yang ada.

3.2 Tabel Penentuan RPN

RPN	Calculating Level
0-25	Very Low
26-50	Low

RPN	Calculating Level
51-75	Medium
76-100	High
>100	Very High

6. **Penentuan *rank* risiko** dilakukan dengan mengurutkan seluruh risiko mulai dari yang memiliki nilai RPN terbesar hingga terkecil.
7. **Penanganan risiko tindak lanjut** dilakukan dengan menyesuaikan risiko dengan tindak lanjut yang ada di ISO 27001:2022

HASIL DAN PEMBAHASAN

A. Analisis konteks bisnis

Berdasarkan analisis data pada KPU, ruang lingkup pada penelitian ini adalah

1. *Mobile Application* Sirekap
2. *Web Application* KPU yang terfokus pada pemilu pemilu2024.kpu.go.id

B. Identifikasi aset

Dalam menentukan identifikasi aset, akan digunakan 4 kategori seperti tabel di bawah.

4.1 Tabel Identifikasi Aset

Kategori	Aset
People	Panitia penyelenggara pemilu
Data/Informasi	Data pencoblosan
	Data pemilih
Software	*Cloud Server*
	Model OCR
	Mobile Application
	Web Application
Hardware	Server fisik
	Handphone
	Router Wifi

C. Identifikasi risiko

Setelah dilakukan identifikasi aset, didapatkan 5 dari setiap kategori seperti tabel di bawah

4.2 Tabel Identifikasi Risiko

Kode	Asset	Failure Mode	Cause Failure	Effect Failure
PEO-01	People	Pengguna Tidak Mengetahui Cara Penggunaan Aplikasi Sirekap	Kurangnya sosialisasi kepada pengguna Aplikasi Sirekap	Terjadinya salah input data dan memperlambat pekerjaan
PEO-02	People	Panitia tidak memasukkan ulang data di aplikasi	Kurangnya sosialisasi	Data yang dimasukkan tidak sesuai
PEO-03	People	Kamera pengguna / panitia tidak bisa mendeteksi angka OCR yang tertulis di kertas C1	Ketebalan angka kurang	Angka yang masuk tidak sesuai atau tidak bisa di deteksi
PEO-04	People	Angka OCR susah terdeteksi	Panitia tidak bisa mengatur pencahayaan atau fokus kamera saat mengambil gambar	Data yang masuk tidak sesuai atau tidak terdeteksi
PEO-05	People	Kamera pengguna / panitia tidak bisa mendeteksi angka OCR yang tertulis di kertas C1	Kertas terlipat atau kusut	Data yang masuk tidak sesuai
DAIN-01	Information/ Data	Data / Informasi pemilih di curi pihak tidak bertanggung jawab	Pencurian Data / Informasi Pemilih	kepercayaan masyarakat berkurang
DAIN-02	Information/ Data	Rawan ada keasalahan memasukkan data yang disengaja ataupun tidak disengaja	Tidak memiliki fitur Error Checking	Adanya perbedaan data recap suara yang masuk
DAIN-03	Information/ Data	Data Rekap Suara Bermasalah	KPPS tidak dapat mengoreksi data Pilpres yang terbaca salah oleh aplikasi Sirekap. Koreksi di Sirekap hanya dapat dilakukan oleh KPU.	Adanya perbedaan data recap suara yang masuk
DAIN-04	Information/ Data	Data Rekap Suara Bermasalah	surat suara tertukar	suara yang masuk tidak benar
DAIN-05	Information/ Data	Data Rekap Suara Bermasalah	Tulisan dan gambar kerap tidak terdeteksi ketika diunggah	Data yang masuk tidak sesuai

Kode	Asset	Failure Mode	Cause Failure	Effect Failure
SOFT-01	Software	Server dari pemilu melemah / mati	Terlalu banyak akses atau masalah dari pihak ketiga	dapat mengakibatkan layanan atau website menjadi tidak dapat diakses oleh pengguna
SOFT-02	Software	Salah mendeteksi data	Model Machine Learning masih belum bagus / memadai	Hasil yang tidak akurat dan kegaduhan publik
SOFT-03	Software	Hasil yang tidak dapat dilihat publik	Data yang tidak transparan dan kesalahan sistem	Kurang nya kepercayaan terhadap KPU
SOFT-04	Software	Rentan serangan cyber	DoS	Dapat mengganggu atau merusak operasi pemungutan suara.
HARD-02	Hardware	Kendala input data	Handphone yang tidak memadai	Memperlambat pekerjaan dan kamera yang sulit untuk mendeteksi kode optik
HARD-03	Hardware	Akses internet yang tidak memadai	Kurangnya perhatian terhadap layanan internet maupun router di setiap TPS	Gagal mengakses aplikasi maupun upload hasil perhitungan
HARD-04	Hardware	Data di cloud hilang	Backup server fisik yang tidak ada	Seluruh data hilang dan harus dilakukan pemilihan ulang
HARD-05	Hardware	Manipulasi handphone ataupun jaringan internet yang dipakai	Orang yang tidak bertanggung jawab dapat menyusup kedalam perangkat keras	Data inputan dapat dimanipulasi melalui perangkat keras

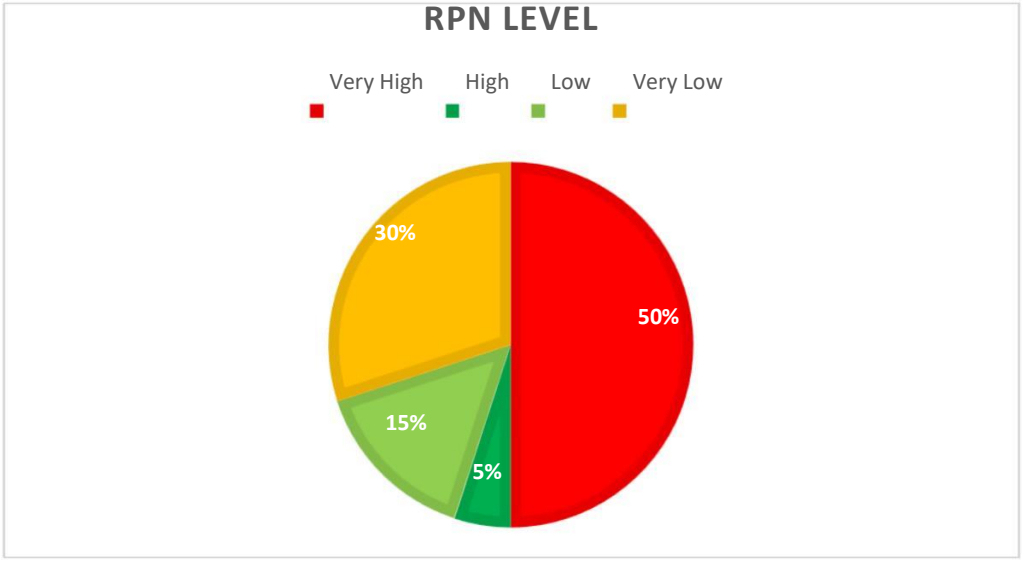
D. Pengelolaan risiko dan Penentuan *Risk Priority Number(*RPN)

Dari 20 risiko yang teridentifikasi, berikut nilai dari Severity (S), Occurrence (O), dan Detection (D) yang didapat berdasarkan hasil observasi dan wawancara. Setelah itu nilai S, O, dan D akan dikalikan untuk mendapatkan nilai RPN.

4.3 Tabel Pengelolaan Risiko dan Penentuan RPN

Kode	Severity (S)	Occurrence (O)	Detection(D)	RPN	Level
PEO-01	7	7	1	49	Low
PEO-02	8	6	1	48	Low
PEO-03	7	6	1	42	Low
PEO-04	8	8	8	512	Very High
PEO-05	6	7	1	42	Low

Kode	Severity (S)	Occurrence (O)	Detection(D)	RPN	Level
DAIN-01	7	8	7	392	Very High
DAIN-02	8	3	5	120	Very High
DAIN-03	8	8	5	320	Very High
DAIN-04	8	7	3	168	Very High
DAIN-05	8	5	1	40	Low
SOFT-01	8	8	2	128	Very High
SOFT-02	8	8	6	384	Very High
SOFT-03	8	1	1	8	Very Low
SOFT-04	8	7	4	224	Very High
SOFT-05	8	8	1	8	Very Low
HARD-01	8	6	2	96	High
HARD-02	7	7	6	294	Very High
HARD-03	8	7	6	336	Very High
HARD-04	8	4	1	32	Low
HARD-05	8	1	1	8	Very Low



E. Penentuan *rank* risiko dan Penanganan risiko tindak lanjut

Setelah mendapatkan nilai RPN, akan diurutkan mulai dari nilai yang terbesar hingga terkecil dan selanjutkan akan dilakukan tindak lanjut sesuai dengan ISO27001:2022

4.4 Tabel Tindak lanjut Risiko

Kode	RPN	Rank	Tindak Lanjut
PEO-04	512	1	7.8 Equipment siting and protection : Peralatan harus ditempatkan dengan aman dan terlindungi
DAIN-01	392	2	5.15 Access control: Meningkatkan mekanisme kontrol akses dan mengimplementasikan sistem pemantauan dan deteksi keamanan yang lebih kuat untuk melindungi data dan informasi pemilih dari akses tidak sah atau pencurian oleh pihak yang tidak bertanggung jawab.
SOFT-02	384	3	5.19 Information security in supplier relationships: Menerapkan prosedur validasi dan verifikasi data yang kuat setelah pemrosesan OCR untuk memastikan keakuratan data yang dikenali, serta memperkuat persyaratan keamanan dan operasional dengan penyedia solusi OCR.
HARD-03	336	4	5.11 Supporting utilities: Mengimplementasikan solusi seperti menyediakan router sendiri ataupuun konektivitas internet dari penyedia layanan untuk memastikan ketersediaan layanan internet yang terus menerus dan memadai.
DAIN-03	320	5	5.19 Information security in supplier relationships: Proses dan prosedur harus ditetapkan dan diterapkan untuk mengelola risiko keamanan informasi yang terkait dengan penggunaan pemasok data atau layanan.
HARD-02	294	6	5.13 Equipment maintenance: Melakukan peningkatan perangkat keras pada perangkat yang digunakan untuk input data atau menggantinya dengan model yang lebih canggih yang mampu menghandle beban kerja yang diperlukan, serta memastikan pemeliharaan perangkat secara teratur.
SOFT-04	224	7	5.18 Access rights, 5.19 Information security in supplier relationships, 5.23 Information security for use of cloud services: Mengimplementasikan kebijakan keamanan yang baik, yang meliputi enkripsi kuat, autentikasi multi-faktor, pemantauan dan respons insiden keamanan.
DAIN-04	168	8	7.10 Storage media: Melakukan pengecekan ulang media penyimpanan yang digunakan untuk memastikan surat suara yang ada
SOFT-01	128	9	5.30 ICT readiness for business continuity: Membangun dan menguji rencana kelangsungan operasional yang komprehensif

Kode	RPN	Rank	Tindak Lanjut
			untuk memastikan bahwa infrastruktur server dapat segera dipulihkan atau digantikan dalam keadaan darurat atau kegagalan sistem.
DAIN-02	120	10	5.30 ICT readiness for business continuity: Membangun dan menguji rencana kelangsungan operasional yang komprehensif untuk memastikan bahwa infrastruktur server dapat segera dipulihkan atau digantikan dalam keadaan darurat atau kegagalan sistem.
HARD-01	96	11	5.30 ICT readiness for business continuity: Melakukan audit dan optimasi infrastruktur server secara berkala untuk memastikan waktu akses yang cepat dan menghindari kegagalan yang bisa menghambat kinerja atau ketersediaan server.
PEO-01	49	12	6.3 Information security awareness, education, and training : Harus mengembangkan dan menyelenggarakan sesi pelatihan yang baik, serta menyediakan dukungan berkelanjutan dan materi pelatihan yang mudah diakses untuk semua pengguna.
PEO-02	48	13	6.3 Information security awareness, education, and training : Harus mengembangkan dan menyelenggarakan sesi pelatihan yang baik, serta menyediakan dukungan berkelanjutan dan materi pelatihan yang mudah diakses untuk semua pengguna.
PEO-03	42	14	5.19 Information security in supplier relationships: Menerapkan prosedur validasi dan verifikasi data yang kuat setelah pemrosesan OCR untuk memastikan keakuratan data yang dikenali, serta memperkuat persyaratan keamanan dan operasional dengan penyedia solusi OCR.
PEO-05	42	15	7.8 Equipment siting and protection : Peralatan harus ditempatkan dengan aman dan terlindungi
DAIN-05	40	16	5.30 ICT readiness for business continuity: Membangun dan menguji rencana kelangsungan operasional yang komprehensif untuk memastikan bahwa infrastruktur server dapat segera dipulihkan atau diga
HARD-04	32	17	5.23 Information security for use of cloud services: Meningkatkan kebijakan dan prosedur pencadangan dan pemulihan data untuk memastikan bahwa semua data penting yang disimpan di cloud memiliki backup yang teratur dan teruji, serta mengaudit dan memperkuat kontrak dengan penyedia layanan cloud untuk memasukkan perjanjian tentang keamanan dan pemulihan data.
SOFT-03	8	18	5.24 Information security incident management planning and preparation: Mengembangkan dan mengimplementasikan prosedur pengelolaan insiden untuk memastikan bahwa masalah teknis yang menghambat publikasi hasil pemilu dapat diidentifikasi dan diatasi secara cepat untuk memulihkan akses publik ke informasi tersebut.

Kode	RPN	Rank	Tindak Lanjut
SOFT-05	8	19	5.18 Access rights: Meninjau dan memperkuat kebijakan pengelolaan peran dan hak akses pengguna untuk memastikan bahwa peran pengguna didefinisikan dengan jelas dan diterapkan dengan tepat.
HARD-05	8	20	5.20 Addressing information security within supplier agreements, 5.16 Identity management and authentication controls: Mengimplementasikan enkripsi kuat dan otentikasi dua faktor pada semua perangkat bergerak dan mengaudit penyedia layanan jaringan untuk memastikan mereka memiliki pengamanan yang memadai terhadap manipulasi

KESIMPULAN

Penelitian ini menunjukkan bahwa penerapat standar ISO 27001:2022 dalam manajemen risiko keamanan informasi di KPU efektif dalam mengidentifikasi dan mengelola risiko yang berkaitan dengan informasi sensitif. Melalui metode Failure Mode and Effects Analysis (FMEA), penlitian ini berhasil mengidentifikasi 20 risiko utama yang mana 50% diantaranya memiliki level very high. Risiko dengan nilai RPN tertinggi, seperti masalah deteksi angka OCR dan pencurian data pemilih, membutuhkan tindakan tindak lanjut yang sesuai dengan standar ISO27001:2022. Dengan implementasi yang tepat, KPU diharapkan dapat meningkatkan mekanisme kontrol akses, validasi data, pemeliharaan perangkat keras, dan keberlanjutan operasional. Penelitian ini memberikan kerangka kerja yang komprehensif bagi KPU dan organisasi lain untuk meningkatkan keamanan informasi dan mengurangi potensi kerugian akibat serangan siber dan kebocoran data.

DAFTAR PUSTAKA

Fuad Amirullah, Syariful Alam, and M.Imam Sulistyo S. 2023. “Analisis Sentimen Terhadap Kinerja KPU Menjelang Pemilu 2024 Berdasarkan Opini Twitter Menggunakan Naïve Bayes.” *STORAGE: Jurnal Ilmiah Teknik Dan Ilmu Komputer* 2 (3). https://doi.org/10.55123/storage.v2i3.2293.

Gauru, Christiana Cristin, Rina Martini, and Laila Kholid Alfirdaus. 2022. “IMPLEMENTASI SIREKAP DALAM PILKADA 2020 KABUPATEN SEMARANG.” *REFORMASI* 12 (2). https://doi.org/10.33366/rfr.v12i2.3874.

Hanifah, Puja, and Jarot S Suroso. 2020. “Analisis Risiko Sistem Informasi Pada RSIA Eria Bunda Menggunakan Metode FMEA.” *Jurnal Komputer Terapan* 6 (2). https://doi.org/10.35143/jkt.v6i2.3728.

Kurniawan, Ade Wahyu, and Muhammad Salman. 2023. “Recommendations for Designing Information Security Framework in Government Procurement of Goods/Services Certification Systems Based on ISO 27001:2022.” *Gema Wiralodra* 14 (2). https://doi.org/10.31943/gw.v14i2.477.

Nurillah, Rifda Aisy, and Agus Trihandoyo. 2024. “Analisis Faktor-Faktor Keamanan Informasi Perusahaan Dalam Penerapan Bring Your Own Device (BYOD).” *IKRA-ITH*

Informatika : Jurnal Komputer Dan Informatika 8 (2). https://doi.org/10.37817/ikraith-informatika.v8i2.2973.

Sinaga, Rudolf. 2024. "Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001:2022." *Jurnal Teknik Informatika Dan Sistem Informasi* 9 (3). https://doi.org/10.28932/jutisi.v9i3.6850.