JSITIK, Vol.3 No.2 Juni 2025
ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

Analisis Risiko Website Sistem Keamanan Informasi Menggunakan Metode Fmea dan Framework ISO/IEC 27002:2022

Diterima:
21 Mei 2025
Revisi:
21 Juni 2025
Terbit:
30 Juni 2025

Maha Shelin Sahira, Rini Indriati, Aidina Ristyawan
Universitas Nusantara PGRI Kediri

Abstrak — Latar Belakang: Keamanan informasi digital menjadi isu penting di era serangan siber yang semakin meningkat. Website RadarKediri.id sebagai portal berita lokal juga rentan terhadap berbagai ancaman keamanan. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis potensi risiko keamanan informasi yang ada. **Tujuan:** Untuk mengetahui risiko-risiko keamanan informasi pada website RadarKediri.id dan memberikan rekomendasi pengendalian risiko berdasarkan standar internasional. **Metode:** Penelitian ini merupakan studi kualitatif yang menggunakan metode Failure Mode and Effect Analysis (FMEA) untuk analisis risiko serta framework ISO/IEC 27002:2022 untuk evaluasi kontrol keamanan. **Hasil:** Ditemukan dua risiko dengan tingkat tinggi, enam risiko sedang, dan dua risiko sangat rendah. Evaluasi efektivitas kontrol berdasarkan 37 kontrol ISO/IEC 27002:2022 menghasilkan skor sebesar 74%, yang masuk kategori "kurang baik, perlu perbaikan". Aspek yang paling memerlukan peningkatan adalah backup data, pemantauan log aktivitas, dan pengendalian hak akses. **Kesimpulan:** Sistem keamanan informasi pada RadarKediri.id masih memiliki kelemahan yang signifikan. Kombinasi metode FMEA dan standar ISO/IEC 27002:2022 terbukti efektif dalam mengidentifikasi celah dan memberikan arahan perbaikan. Penelitian selanjutnya disarankan untuk menerapkan kontrol secara langsung dan mengukur dampaknya secara kuantitatif.
Kata kunci: FMEA; ISO/IEC 27002:2022; Keamanan Informasi; Analisis Risiko

Abstract — Background*:Digital information security has become a crucial issue amid the rising number of cyberattacks. The website RadarKediri.id, as a local news portal, is also vulnerable to various security threats. This study aims to identify and analyze potential information security risks.* ***Objective:*** *To identify information security risks on the RadarKediri.id website and provide risk control recommendations based on international standards.* ***Method:*** *This is a qualitative study using the Failure Mode and Effect Analysis (FMEA) method for risk analysis and the ISO/IEC 27002:2022 framework for evaluating security controls.* ***Results:****The analysis found two high-level risks, six medium-level risks, and two very low-level risks. The evaluation of control effectiveness based on 37 ISO/IEC 27002:2022 controls yielded a score of 74%, which falls into the category of "poor, needs improvement." The most critical areas for improvement are data backup, activity log monitoring, and access rights control.* ***Conclusion:*** *The information security system on RadarKediri.id still has significant weaknesses. The combination of FMEA and the ISO/IEC 27002:2022 standard proved effective in identifying gaps and providing recommendations for improvement. Future research is recommended to implement the proposed controls and quantitatively assess their impact.*
Keywords: *FMEA; ISO/IEC 27002:2022; Information Security; Risk Analysis*

Penulis Korespondensi:

Maha Shelin Sahira,
Sistem Informasi,
Universitas Nusantara PGRI Kediri,
Email: shellinsahira@gmail.com

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

I. PENDAHULUAN

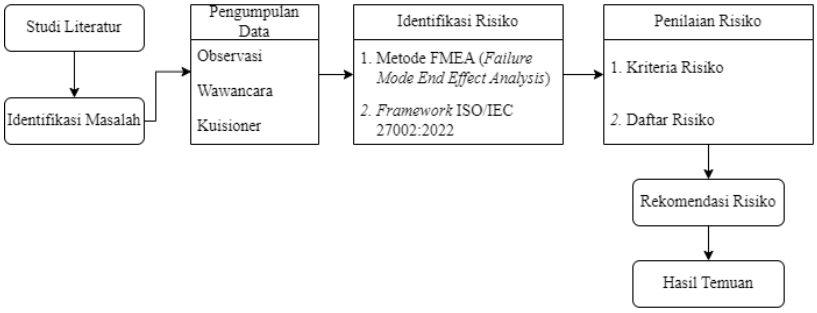
Dalam era digital yang semakin berkembang, informasi telah menjadi salah satu aset penting bagi organisasi. Keamanan informasi tidak hanya berkaitan dengan perlindungan data dari akses yang tidak sah, tetapi juga mencakup upaya untuk menjaga keberlangsungan operasional organisasi dari ancaman internal maupun eksternal. [1] Risiko yang berkaitan dengan sistem informasi dapat berasal dari berbagai faktor, seperti serangan *siber*, kesalahan manusia, maupun kegagalan teknologi, yang dapat mengakibatkan kerugian signifikan apabila tidak dikelola dengan baik [2]. Pengukuran risiko pada keamanan informasi memiliki peran penting dalam menjaga keberlangsungan operasional sistem informasi dengan cara mengidentifikasi, menganalisis, dan mengklasifikasikan berdasarkan tingkat dampak keparahan risiko terhadap keberlangsungan operasional dampak keparahan risiko [3]. Namun, hingga saat ini belum ditemukan penelitian yang secara spesifik mengkaji risiko keamanan informasi pada website RadarKediri.id menggunakan pendekatan gabungan FMEA dan ISO/IEC 27002:2022. Perbedaan penelitian ini dengan penelitian sebelumnya adalah penggunaan kombinasi metode FMEA dan framework ISO/IEC 27002:2022 dalam konteks sistem keamanan informasi (RadarKediri.id), yang belum pernah dikaji secara menyeluruh. Tujuan penelitian ini adalah untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko keamanan informasi pada website RadarKediri.id serta memberikan rekomendasi mitigasi berdasarkan framework ISO/IEC 27002:2022.

Dampak kegagalan sistem dapat menghambat keberlangsungan operasional berpotensi menimbulkan kerugian yang signifikan, [4] upaya ini difokuskan pada kegagalan sistem diperusahaan Radar Kediri yang sebelumnya website belum pernah dilakukan penelitian terhadap analisis terjadinya kegagalan sistem. [5] dengan penerapkan proses identifikasi dan pegendalian risiko secara lebih sistematis dapat diperlukan pendekatan penilaian risiko yag struktur seperti metode FMEA (*failure mode and effect analysis*) yang dapat mengukur tingkat keparahan, kemukinan terjadinya risiko dan deteksi dari setiap potensi kegagalan sistem. [6]dari hasil penilaian yang diperoleh dapat digunakan sebagai dasar dalam merumuskan rekomendasi pengendalian keamanan dengan kode praktik pada *framework* ISO/IEC 27002:2022 sebagai bahan rekomendasi pengendalian risiko [7].

JSITIK, Vol.3 No.2 Juni 2025
ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

II. METODE

Pada bagian ini berisi penjelasan tentang jenis penelitian/desain penelitian.



Gambar 1. Metode Penelitian

Gambar 1. Menjelaskan tentang metode penelitian yang digunakan dalam mengidentifikasi keamanan sistem informasi. Tujuannya untuk menganalisis sebagaimana website terdampak pada kebocoran sistem. Berikut adalah penjelasan dari alur kinerja metode penelitian.

II.1 Studi Literatur

Mengkaji teori-teori, metode yang akan digunakan dan standar prosedur yang relevan dalam penelitian seperti langkah-langkah penyelesaian risiko dalam sebuah website yang bertujuan agar memiliki landasan yang lebih terperinci dan sistematis

II.2 Identifikasi Masalah

Tahapan ini menentukan permasalaahan yang akan di analisis dalam penelitian yang bertujuan untuk menemukan dan merumuskan masalah yang akan diselesaikan. Pada tahap identifikasi masalah ini peneliti dapat menguraikan masalah berdasarkan kuisioner, observasi dan wawancara.

II.3 Pengumpulan Data

a). Observasi

Observasi adalah metode pengumpulan data yang dilakukan dengan cara mengamati langsung objek yang sedang diteliti. Peneliti mencatat aktivitas atau kondisi tertentu tanpa intervensi langsung sehingga data dapat diperoleh secara alami dnegan situasi kejadian yang sebenarnya.

b). Wawancara

Wawancara adalah suatu teknik pengumpulan data yang dilakukan melalui interaksi antara peneliti dan responden. Dengan tujuan untuk menemukan suatu informasi, pendapat, dan pengalaman lebih mendalam tentang pertanyaan yang akan disampaikan peneliti.

c). Kuisioner

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

Kuisioner merupakan teknik pengumpulan data informasi untuk menganalisis proses terjadinya risiko dalam suatu organisasi yang bisa berpengaruh oleh sistem terkait data kuisioner yang diajukan.

II.4 Identifikasi risiko

a). Metode FMEA

Metode FMEA (*failure mode and effect analysis*) merupakan metode terstruktur untuk mengidentifikasi dan menghindari mode kegagalan. Dampak yang terjadi menggunakan skala prioritas[8]. FMEA bertujuan untuk mengkaji suatu proses guna mengidentifikasi kemungkinan terjadinya kegagalan, menganalisis dampak timbul, serta probabilitas terjadinya kegagalan sistem [9]

b). *Framework* ISO/IEC 27002:2022

ISO/IEC 27002 merupkan dokumen yang disetujui sebagai panduan praktik dalam penerapan kontrol keamanan informasi. Tujuannya sebagai kontrol organisasi yang dapat melaksanakan langkah-langkah perlindungan yang efektif untuk mencapai sasaran ISO/IEC 27001[10]. Panduan ini juga dapat dijadikan acuan dalam melakukan analisis mengenai kontrol yang diterapkan. Namun, karena bersifat sebagai pedoman, ISO/IEC 27002 tidak dapat digunakan sebagai dasar sertifikasi [11]

II.5 Penilaian risiko

Penilaian risiko dilakukan setelah penyebaran kuesioner menggunakan metode FMEA: dampak keparahan (*severity*), kemungkinan kejadian (*occurrence*), dan kemampuan deteksi (*detection*). [12] untuk menentukan tingkat prioritas risiko (RPN) setiap kegagalan sistem, menggunakan rumus RPN = Dampak Keparahan (S) x Kejadian(O) x Deteksi(D).[13]

a). Skala Risiko *Severity*

Tabel 2. 1 Severity

Tingkat Keparahan	***Severity***	**Deskripsi**
10	Berbahaya tanpa peringatan	Kegagalan total pada sistem yang menimbulkan dampak berbahaya
9	Berbahaya dengan peringatan	Kegagalan sistem yang menyebabkan risiko tinggi yang masih bisa terdeteksi sebelumnya
8	Sangat parah	Sistem mengalami kegagalan total dan tidak dapat berfungsi
7	Parah	Sistem masih dapat berjalan, tetapi terdeteksi gangguan yang signifikan

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

6	Sedang	Sistem dapat beroperasi, namun terdapat penurunan peforma yang berdampak pada hasil
5	Menengah	Kinerja menurun secara bertahap, namun tidak mengganggu fungsi utama
4	Rendah	Dampak kegagalan tidak terlalu signifikan, hanya mengurangi peforma
3	Sangat rendah	Dampak kegagalan kinerja sistem tergolong kecil
2	Kecil kemungkinan	Dampak kegagalan sangat kecil, dan hamper tidak berpengaruh pada sistem
1	Tidak berpengaruh	Tidak ada pengaruh kegagalan terhadap kinerja sistem

b). Skala Risiko *Occurance*

Tabel 2.2 *Occurance*

Tingkat Keparahan	***Occurance***	**Deskripsi**
10 - 9	Sangat tinggi	Kegagalan sering terjadi
8 - 7	Tinggi	Gangguan muncul berulang dalam jangka waktu tertentu
6 - 4	rendah	Jarang terjadi kegagalan
3 - 2	Sangat rendah	Kemungkinan terjadi kegagalan sangat rendah
1	Tidak berpengaruh	Hampir tidak mengalami kegagalan

c). Skala Risiko *Detection*

Tabel 2.3 *Detection*

Tingkat Keparahan	***Detection***	**Deskripsi**
10	Tidak terdeteksi	Risiko habis tidak bisa ditemukan
9	Hampir tidak terdeteksi	Sangat sulit menemukan risiko
8	Sangat rendah terdeteksi	Risiko sulit terdeteksi
7	Rendah terdeteksi	Sistem deteksi lemah, atau tidak dapat mengenali sebagian jenis kegagalan.
6	Sedang kemungkinan terdeteksi	Deteksi hanya dilakukan pada sampel, bukan menyeluruh, sehingga ada risiko kegagalan tidak terdeteksi dan tetap lolos proses.
5	Cukup tinggi terdeteksi	Ada prosedur deteksi, tetapi tidak 100% akurat atau tidak dilakukan secara rutin.
4	Tinggi terdeteksi	Risiko cukup mudah terdeteksi/ditemukan

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

3	Sangat tinggi tekdeteksi	Risiko mudah ditemukan dengan pengujian
2	Sangat mungkin terdeteksi	Deteksi risiko hampir selalu berhasil melalui sistem kontrol yang kuat dan rutin pemeriksaan manual.
1	Sangat terdeteksi	Sistem deteksi hampir selalu menemukan kegagalan. Ada kontrol otomatis, pengujian 100% sehingga kegagalan tidak terdeteksi sangat kecil.

II.6 Rekomendasi risiko

Rekomendasi risiko menggunakan prosedur *Framework* ISO/IEC 27002:2022 dengan menggunakan klausa yaitu Keamanan informasi. *framework* iso/iec 27002:2022 tentang struktur standar iso/iec yang memiliki 4 klausa dari setiap klausa memiliki beberapa kontrol keamanan kebutuhan untuk keamanan informasi. [14]

III. HASIL DAN PEMBAHASAN

Pengukuran risiko terhadap keamanan informasi ini dilakukan dengan menggunakan metode FMEA dihitung antara probabilitas tingkat *Severity* (S), *Occurrence* (O), *Detection* (D) yaitu RPN (*Risk Priority Number*) = S × O × D yang akan dievaluasi dengan menggunakan 10 point skala RPN

Tabel 3.1 Skala RPN

Level Risiko	Skala Nilai RPN	Deskripsi
Sangat rendah	$X < 50$	Risiko dapat diterima
Rendah	$50 \leq X < 100$	Perlu pemantauan ringan
Sedang	$100 \leq X < 150$	Perlu tindakan secara berkala
Tinggi	$150 \leq X < 250$	Perlu tindakan migrasi segera
Sangat tinggi	$X \geq 250$	Harus ditangani sesegera mungkin

Daftar potensi kegagalan dalam bentuk pengumpulan data dari skala RPN frekuensi kejadian (Occurance), penentuan ringkat keparahan (severity), serta mengidentifikasi peyebab kejadian(Detection) dan penvegahan dari masing-masing mode kegagalan. metode ini sebagai tolak ukur untuk memnentukan prioritas dampak kegagalan sistem yang akan ditindaklanjuti.[15]

Tabel 3.2 Daftar Risiko

NO	Potensi Risiko	Penyebab Risiko	NS	NO	ND	RPN	Level Risiko
1	Terdapat peretasan pada server dan website	Server dan website dikelola oleh tim teknis yang kurang memahami keamanan siber	8	4	6	192	Tinggi
2	Audit keamanan tidak terdokumentasi dan tidak ditindaklanjuti	Belum pernah dilakukan audit pada keamanan	7	5	5	175	Tinggi
3	Data backup tidak tersedia pada saat sistem rusak	Backup hanya dilakukan secara manual dan tidak otomatis, serta hanya	7	4	5	140	Sedang

JSITIK, Vol.3 No.2 Juni 2025
ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

		disimpan dilokasi yang sama dengan server utama					
4	Aktivitas mencurigakan tidak dapat terdeteksi	Belum diterapkan sistem pemrosesan log yang mendukung deteksi terhadap aktifikas yang mencurigakan.	5	7	4	140	Sedang
5	Rusaknya aset server IT	Aset server rusak terjadi karena bencana alam, kesalahan operasional	8	4	4	128	Sedang
6	Perubahan berita penting atau login tidak tercatat	Tidak adanya kebijakan atau prosedur pencatatan log aktivitas penting	6	5	4	120	Sedang
7	Kebocoran data atau aset yang tidak terpakai/rusak	Penetapan dan pembuangan aset tidak sesuai dengan prosedur, maka keboran data bisa terjadi	7	4	4	112	Sedang
8	Terjadikan kesalahan hak akses pada data yang tersimpan pada ruang penyimpanan	User dan password hak akses dibagikan kepada orang lain tanpa sepengetahuan pihak IT dalam pemberian hak akses	5	5	4	100	Sedang
9	Website tidak dapat diakses terjadi kesalahan	Website tidak memiliki cadangan sistem jika server utama bermasalah.	4	3	3	36	Sangat rendah
10	Tidak memiliki staf pada bidang IT keamanan	Kurangnya tenaga staf pada bidang IT khususnya keamanan	4	3	3	36	Sangat rendah

Pada temuan dari daftar risiko untuk melakukan rekomendasi pengananan yaitu terdapat 2 level tinggi, dan 6 level sedang. Setelah melakukan pemetaan pada risiko keamanan website menggunakan prosedur ISO/IEC 27002:2022, langkah selanjutnya yaitu rekomendasi penentuan untuk menanggani risiko-risiko yang sudah terjadi dengan menggunakan kontrol ISO/IEC 27002:2022

Tabel 3.3 Rekomendasi ISO/IEC 27002:2022

No	Potensi risiko	Penyebab risiko	RPN	Kontrol ISO/IEC 27002:2022	Rekomendasi penanganan risiko
1	Terdapat peretasan pada server dan website	Server dan website dikelola oleh tim teknis yang kurang memahami keamanan siber	192	5.7 *Threat Intelligence*	• Melakukan monitoring server dan website secara aktif • Memperbarui kebijakan keamanan informasi, dan melakukan audit keamanan berkala.
2	Audit keamanan tidak	Belum pernah dilakukan audit pada keamanan	175	5.35 *Independent Review of*	• Membentuk tim audit internal atau menggunakan auditor eksternal independen,

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

	terdokumentasi			*Information Security*	• Mendokumentasikan / melaporan semua hasil audit, menetapkan rencana perbaikan.
3	Data backup tidak tersedia pada saat sistem rusak	Backup dilakukan secara manual, serta disimpan dilokasi yang sama dengan server utama	140	8.13 *Information Backup*	• Mengimplementasikan sistem backup otomatis dengan penyimpanan offsite/cloud • Melakukan pengujian pemulihan data secara berkala sesuai kebijakan backup secara rutin.
4	Aktivitas mencurigakan tidak dapat terdeteksi	Belum diterapkan sistem pemrosesan log yang mendukung deteksi terhadap aktifikas yang mencurigakan.	140	8.16 *Monitoring activities* 8.28 *Secure Coding*	• Melakukan implementasi SIEM(*Security Information and Event Management*) untuk pemantauan, • Menerapkan prosedur audit log terkait monitoring, pelaporan insiden.
5	Kebocoran data atau aset yang tidak terpakai/ rusak	Penetapan pembuangan aset tidak sesuai dengan prosedur, maka keboran data bia terjadi	112	7.14 – *Secure Disposal or Re-use of Equipment*	Menerapkan secure coding dan melakukan code review untuk menghindari kelemahan pada kode program
6	Rusaknya aset server IT	Aset server rusak terjadi karena bencana alam, kesalahan operasional	128	7.5 – *Protecting against physical and environmental threats*	• Melakukan wiping data menggunakan tools standar keamanan • Membuat kebijakan formal untuk disposal dan reuse perangkat TI.
7	Perubahan berita penting atau login tidak tercatat	Tidak adanya kebijakan atau prosedur pencatatan log aktivitas penting	120	8.15 – *Logging*	Membuat kebijakan internal yang mewajibkan pencatatan dan penyimpanan log minimal selama 3–6 bulan.
8	Terjadikan kesalahan hak akses pada data yang tersimpan pada ruang penyimpanan,	User dan password hak akses dibagikan kepada orang lain tanpa sepengetahuan pihak IT	100	5.15 – *Access Control* 5.18 – *Access Rights*	• Batasi akses dari perangkat, implementasikan otentikasi dua faktor untuk login • Memverifikasi bahwa tingkat akses yang diberikan sesuai dengan kebijakan topik-spesifik tentang kontrol akses

Hasil temuan penelitian ini mencakup dalam proses perencanaan stategi yang terdapat evaluasi hasil kinerja untuk mengidentifikasi risiko.

Tabel 3.4 Hasil Temuan

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

No	Kontrol organisasi	1	2	3	4	5
1	5.7 *Threat Intelligence*				✓	
2	5.35 *Independent review information security*					✓
3	8.13 *Information Backup*			✓		
4	8.28 *Secure Code*			✓		
5	8.16 *Monitoring activities*			✓		
6	7.14 *Secure Disposal or Re-use of Equipment*				✓	
7	7.5 *Protecting against physical and environmental threats*					✓
8	5.15 *Access Control*				✓	
9	5.18 *Access Rights*			✓		
10	8.15 – *Logging*			✓		

Keterangan :

1 = Sudah tersedia dan berjalan dengan baik

2 = Sudah tersedia, tetapi penerapannya belum konsisten

3 = Sudah tersedia, namun masih dalam perbaikan

4 = Belum tersedia, tetapi telah masuk dalam rencana

5 = Belum tersedia dan belum direncanakan

Rumus presense kontrol :

$$presense\ \frac{jumlah\ skor\ aktual}{jumlah\ skor\ maksimal}\ X\ 100 \qquad (1)$$

Perhitungan :

$$\frac{37}{50} \times 100 = 74\%$$

Hasil dari presense hasil temuan :

1 – 30% = Sangat Baik

31 – 60% = Baik, namun perlu peningkatan

61 – 85% = Kurang baik, perlu perbaikan

86 – 100% = Sangat buruk, perlu perhatian khusus

Pada hasil diatas yaitu “74%” yang dinyatakan “kurang baik, perlu perbaikan”. Dapat disimpulkan bahwa dari hasil penilaian risiko, mengevaluasi tingkat keparahan risiko sampai merekomendasikan menggunakan kontrol ISO/IEC 27002:2022. Pada website RadarKediri.id masih membutuhkan audit untuk mengevaluasi segala risiko yang terjadi dan monitoring sistem secara berkala untuk menjaga keamanan berkelanjutan.

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

IV. KESIMPULAN

Kesimpulan peneliti untuk website RadarKediri.id masih memiliki kelemahan dalam aspek keamanan karena terdapat temuan belum pernah dilakukan audit keamanan website. Hal ini dapat diungkap melalui proses observasi, wawancara dan kuisioner yang digunakan untuk mengidentifikasi risiko. Menggunakan metode FMEA (*Failure Mode And Effect Analysis)* menunjukan bahwa ditemukan 2 resiko level tinggi, 6 risiko level sedang dan 2 reisiko levek sangat rendah artinya sistem masih rentan terdahap gangguan dan perlu pengananan. Untuk penanganan risiko peneliti menggunakan rekomendasi dari *Framework* ISO/IEC 27002:2022 dari rekomendasi hasil temuan kini tercapai 74% tingkatan, penerapan kontrol masih belum optimal dan perlu ditingkatkan. Dengan menggabungkan metode FMEA dan ISO/IEC 27002:2022, sistem keamanan dapat diperkuat secara terstruktur

DAFTAR PUSTAKA

[1] A. C. Zarkasi, A. S. Wardani, and S. Sucipto, "Analisa User Experience Terhadap Fitur Di Aplikasi Zenius Menggunakan Heart Framework," METHOMIKA J. Manaj. Inform. dan Komputerisasi Akunt., vol. 6, no. 6, pp. 174–179, 2022, doi: 10.46880/jmika.vol6no2.pp174-179.

[2] F. S. Wati, D. A. Prambudi, and H. I. Sunardi, "Evaluasi Keamanan Informasi di Universitas XYZ Dengan Menggunakan Indeks KAMI 4 . 2," vol. 2, no. 1, pp. 1–7, 2024.

[3] I. Shahroini, R. Indriati, and T. Andriyanto, "Sistem Informasi Manajemen Bantuan Sosial Desa," Agustus, vol. 7, pp. 2549–7952, 2023.

[4] A. Ramadhani, "Keamanan Informasi," Nusant. - J. Inf. Libr. Stud., vol. 1, no. 1, p. 39, 2018, doi: 10.30999/n-jils.v1i1.249.

[5] F. Ardiansyah, A. S. Wardani, and S. Sucipto, "Rancang Bangun Company Profile Pusat Pelayanan Terpadu Perlindungan Perempuan dan Anak Berbasis Website," JSITIK J. Sist. Inf. dan Teknol. Inf. Komput., vol. 1, no. 2, pp. 124–136, 2023, doi: 10.53624/jsitik.v1i2.176.

[6] M. Huda, A. S. Wardani, E. Daniati, and R. Firliana, "Analisa Tata Kelola Sistem Informasi Administrasi Kependudukan (SIAK) Menggunakan Framework COBIT 5 Domain DSS02," 2020.

[7] M. I. P. Sirait, N. I. S., & Nasution, "PENTINGNYA SISTEM INFORMASI AUDIT DALAM MENINGKATKAN KEAMANAN DATAPERUSAHAAN," vol. 5, no. 4, pp. 1–23, 2024, [Online]. Available: https://ejournal.warunayama.org/index.php/kohesi/article/view/7451

[8] Y. Ramayani, "Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA)," INOVTEK Polbeng - Seri Inform., vol. 7, no. 2, p. 289, 2022, doi: 10.35314/isi.v7i2.2631.

[9] T. Widianti and D. Sih, "FAILURE MODE AND EFFECT ANALYSIS (FMEA) SEBAGAI TINDAKAN PENCEGAHAN PADA KEGAGALAN PENGUJIAN," no. January 2020, pp. 250–260, 2020.

[10] Ardhana Yudi Saputra, "PEMBUATAN STANDAR OPERATING PROCEDURE KEAMANAN ASET INFORMASI BERDASARKAN KENDALI AKSES DENGAN MENGGUNAKAN ISO/IEC:27002:2013 PADA STUDI KASUS STIE PERBANAS SURABAYA," 2020.

[11] D. Fatih and R. Fathoni Aji, "Evaluasi Keamanan Informasi Menggunakan ISO/IEC 27001: Studi Kasus PT XYZ," J. Sains Komput. Inform. (J-SAKTI, vol. 8, no. 1, pp. 72–

ISSN: 2986-0458 (Print) / 2986-044X (Online)
DOI: https://doi.org/10.53624/jsitik.v3i2.722

84, 2024.
[12] N. Matondang, I. N. Isnainiyah, and A. Muliawatic, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)," J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 2, no. 1, pp. 282–287, 2018, doi: 10.29207/resti.v2i1.96.
[13] D. I. Situngkir, "Pengaplikasian FMEA untuk Mendukung Pemilihan Strategi Pemeliharaan pada Paper Machine," FLYWHEEL J. Tek. Mesin Untirta, vol. 1, no. 1, p. 39, 2020, doi: 10.36055/fwl.v1i1.5489.
[14] Muhamad Rifqi Fadli, "Analisa penerapan sistem manajemen keamanan informasi berdasarkan iso 27001:2022 di pusat data dan sistem informasi badan standarisasi nasional," pp. 1–23, 2024.
[15] H. I. Pribadi and E. Ernastuti, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina)," J. Sist. Inf. Bisnis, vol. 10, no. 1, pp. 28–35, 2020, doi: 10.21456/vol10iss1pp28-35.