Saturnus : Jurnal Teknologi dan Sistem Informasi
Volume. 3, Nomor. 3, Juli 2025
e-ISSN : 3031-9943; dan p-ISSN : 3031-9935; Hal. 136-154
DOI: https://doi.org/10.61132/saturnus.v3i3.983
Available online at: https://journal.arteii.or.id/index.php/Saturnus

Analisis Risiko Keamanan Siber Website Peken Surabaya Menggunakan Standar ISO 27005:2019 dan OWASP ZAP

Cynthia Widya Lestari[1], Nurul Izzah[2], Puti Tsabita Najwa Arief[3], Muhammad Ananda Giovanny R[4], Agung Brastama Putra[5]
[1-5] Universitas Pembangunan Nasional Veteran Jawa Timur, Indonesia

Email: 22082010045@student.upnjatim.ac.id, 22082010046@student.upnjatim.ac.id, 22082010048@student.upnjatim.ac.id, 22082010110@student.upnjatim.ac.id, agungbp.si@upnjatim.ac.id

Korespondensi penulis: 22082010046@student.upnjatim.ac.id

Abstract. *The rapid growth of information technology has driven digital transformation in various sectors, including micro, small, and medium enterprises (MSMEs), the backbone of the Indonesian economy. In response to the challenges and opportunities of digitalization, the Surabaya City Government launched the Peken e-commerce platform on October 31, 2021. This platform aims to help MSMEs market their products online, expand market reach, and increase competitiveness. However, the use of digital systems also presents new challenges, particularly in terms of cybersecurity. Dependence on technology opens the door to various threats that can compromise data confidentiality, integrity, and availability. This study aims to analyze and evaluate information security risks on the Peken Surabaya website using a risk management approach based on the ISO/IEC 27005:2019 standard. The analysis method involves identifying information assets, recognizing potential threats, identifying vulnerabilities, and assessing risk levels based on the likelihood of occurrence and impact. To support the analysis, technical testing was also conducted using the Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) tool. The research results indicate that most of the risks faced by Peken Surabaya are moderate to very high. These risks include Distributed Denial of Service (DDoS) attacks, user data leaks, and the lack of a two-factor authentication (2FA) system. Based on these findings, a risk management strategy was developed using the Risk Modification, Risk Sharing, Risk Retention, and Risk Avoidance approaches. Furthermore, this study recommends security controls based on ISO/IEC 27005 and OWASP Top 10 to enhance system protection. These findings emphasize the importance of implementing international standards-based risk management in maintaining the continuity and security of digital public services, particularly those supporting the MSME sector in the digital era.*

Keywords: *Cybersecurity, Risk Analysis, ISO 27005:2019, OWASP ZAP, Peken Surabaya Website.*

Abstrak. Pesatnya pertumbuhan teknologi informasi telah mendorong transformasi digital di berbagai sektor, termasuk sektor usaha mikro, kecil, dan menengah (UMKM) yang merupakan tulang punggung perekonomian Indonesia. Sebagai respons terhadap tantangan dan peluang digitalisasi, Pemerintah Kota Surabaya meluncurkan platform e-commerce Peken pada 31 Oktober 2021. Platform ini bertujuan untuk membantu UMKM dalam memasarkan produk mereka secara daring, memperluas jangkauan pasar, dan meningkatkan daya saing. Namun, pemanfaatan sistem digital juga menghadirkan tantangan baru, khususnya dalam hal keamanan siber. Ketergantungan pada teknologi membuka celah terhadap berbagai ancaman yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan data. Penelitian ini bertujuan untuk menganalisis dan mengevaluasi risiko keamanan informasi pada website Peken Surabaya dengan menggunakan pendekatan manajemen risiko berdasarkan standar ISO/IEC 27005:2019. Metode analisis dilakukan melalui proses identifikasi aset informasi, pengenalan potensi ancaman, identifikasi kerentanan, serta penilaian tingkat risiko berdasarkan kemungkinan terjadinya dan dampak yang ditimbulkan. Untuk mendukung analisis, dilakukan pula pengujian teknis menggunakan alat Open Web Application Security Project Zed Attack Proxy (OWASP ZAP). Hasil penelitian menunjukkan bahwa sebagian besar risiko yang dihadapi Peken Surabaya berada pada tingkat sedang hingga sangat tinggi. Risiko-risiko tersebut meliputi serangan Distributed Denial of Service (DDoS), kebocoran data pengguna, serta ketiadaan sistem autentikasi dua faktor (2FA). Berdasarkan temuan tersebut, disusun strategi penanganan risiko dengan pendekatan Risk Modification, Risk Sharing, Risk Retention, dan Risk Avoidance. Selain itu, penelitian ini juga merekomendasikan kontrol keamanan berdasarkan ISO/IEC 27005 dan OWASP Top 10 untuk meningkatkan perlindungan sistem. Temuan ini menegaskan pentingnya penerapan manajemen risiko yang berbasis standar internasional dalam menjaga keberlangsungan dan keamanan layanan publik digital, terutama yang mendukung sektor UMKM di era digital.

Kata kunci: *Keamanan Siber, Analisis Risiko, ISO 27005:2019, OWASP ZAP, Website Peken Surabaya.*

Received: Juni 15, 2025; Revised: Juni 30, 2025; Accepted: Juli 28, 2025; Published: Juli 31, 2025

1. LATAR BELAKANG

Perkembangan teknologi informasi yang pesat mendorong transformasi digital di berbagai sektor, termasuk UMKM—unit usaha yang memenuhi klasifikasi mikro, kecil, atau menengah yang menjadi tulang punggung perekonomian Indonesia karena menyerap banyak tenaga kerja, meratakan pendapatan, dan menyumbang porsi terbesar terhadap PDB nasional [1]. Besarnya peran ini menuntut pemerintah, pusat maupun daerah, untuk memberi perlindungan, dukungan, dan fasilitas pengembangan yang nyata. Dalam kerangka desentralisasi, pemerintah daerah dipandang paling dekat untuk mengenali dan mengakselerasi potensi UMKM setempat. Surabaya, kota terbesar kedua di Indonesia, menghadapi tantangan ganda: peralihan pola transaksi dari konvensional ke digital dan penurunan pertumbuhan ekonomi pada 2021. Oleh karenanya, berdasarkan Peraturan Daerah Kota Surabaya Nomor 4 Tahun 2021 tentang RPJMD 2021–2026, Pemerintah Kota Surabaya menargetkan transformasi birokrasi yang tangkas dan berbasis digital [2]. Hal ini mendorong pelayanan publik untuk berinovasi secara digital, termasuk dalam mendukung pelaku UMKM. Sebagai bentuk komitmen terhadap ekonomi kerakyatan, Pemkot Surabaya merilis *website e-commerce* bernama Peken (Pemberdayaan lan Ketahanan Ekonomi Nang Suroboyo) pada 31 Oktober 2021, yang berfungsi sebagai platform digital untuk membantu UMKM memasarkan produk secara daring [1]. *Website* ini menjadi media penting dalam mendukung digitalisasi UMKM Surabaya di era ekonomi digital.

Namun, seiring dengan meningkatnya ketergantungan pada sistem digital, risiko terhadap keamanan siber pun menjadi ancaman yang signifikan. Ancaman siber seperti serangan injeksi, pencurian data, atau gangguan layanan dapat berdampak serius pada integritas, ketersediaan, dan kerahasiaan data. Oleh karena itu, diperlukan analisis risiko keamanan informasi yang menyeluruh agar potensi kerentanan dapat diidentifikasi dan dikendalikan secara efektif. ISO/IEC 27005:2019 sebagai standar internasional menyediakan panduan sistematis dalam manajemen risiko keamanan informasi, mulai dari identifikasi aset, ancaman, kerentanan, hingga evaluasi dan penanganan risiko. Untuk mendukung proses ini, OWASP ZAP (*Zed Attack Proxy*) juga digunakan sebagai alat bantu dalam mengidentifikasi kerentanan teknis pada website, seperti *Cross-Site Scripting* (XSS), SQL Injection, dan kerentanan lainnya yang umum terjadi pada *website* [3].

Meskipun telah banyak dilakukan penelitian terkait manajemen risiko keamanan informasi, sebagian besar studi tersebut masih menggunakan ISO 27005 versi sebelumnya (2011 atau 2013), serta belum mengintegrasikan pendekatan teknis menggunakan OWASP

ZAP dalam konteks sistem layanan publik seperti *website* Peken Surabaya. Misalnya, Isnaini et al. (2023) [4] menerapkan ISO 27005:2019 pada sistem pelayanan desa, namun fokusnya terbatas pada gangguan server dan belum menyentuh aspek pengujian teknis berbasis *tools* seperti OWASP ZAP. Di sisi lain, Sati et al. (2023) [5] telah menggunakan OWASP ZAP untuk mengidentifikasi celah keamanan pada aplikasi *web* Resepedia, namun tidak mengaitkannya dengan manajemen risiko berdasarkan ISO 27005. Dengan demikian, hingga saat ini belum ditemukan penelitian yang secara komprehensif menganalisis risiko keamanan siber website layanan publik berbasis ISO 27005:2019 yang dilengkapi dengan hasil uji teknis dari OWASP ZAP untuk *website* Peken Surabaya.

Penelitian ini hadir untuk mengisi celah tersebut, dengan tujuan memberikan pendekatan terintegrasi antara manajemen risiko dan deteksi kerentanan aktual guna meningkatkan keamanan siber *website* Peken Surabaya yang digunakan dalam mendukung UMKM lokal di Surabaya.

2. KAJIAN TEORITIS

ISO 27005:2019 adalah bagian dari keluarga ISO 27005 yang memiliki beberapa kelebihan seperti, mengurangi *vulnerability*, mengurangi *threat*, mengurangi impact dan lainnya. Pendekatan ini juga digunakan dalam konsep manajemen risiko adalah untuk menilai kesesuaian terhadap suatu pihak baik secara internal maupun eksternal dan dapat melihat hasil akhir daftar risiko, daftar ancaman dan daftar keterkaitan antara risiko yang terjadi dengan ancamannya dan bagaimana solusi yang tepat untuk mengatasi resiko tersebut dengan mengacu pada nilai risiko yang telah diperoleh sebelumnya [6].

Beberapa studi menggunakan metode penelitian yang digunakan melibatkan beberapa tahapan penting dalam ISO 27005:2019, dimulai dari penetapan ruang lingkup dan konteks yang jelas sebagai dasar untuk mengidentifikasi, menganalisis, dan mengevaluasi serta menentukan tindakan yang tepat terhadap risiko keamanan informasi [7]. Kemudian OWASP ZAP (*Zed Attack Proxy*) merupakan salah satu alat open-source yang dikembangkan oleh organisasi non-profit *Open Web Application Security Project* (OWASP), yang berfokus pada peningkatan keamanan aplikasi web. Sebagai bagian dari ekosistem OWASP, ZAP dirancang untuk membantu proses pengujian keamanan aplikasi dengan cara mendeteksi celah dan kerentanan yang dapat dieksploitasi oleh penyerang. Alat ini secara luas digunakan dalam pengujian keamanan karena mudah digunakan serta mendukung baik pengujian otomatis maupun manual. Berdasarkan hasil penelitian oleh M. F. A. Ramadhan dan A. S. Ilmananda

[8], OWASP ZAP digunakan untuk menganalisis keamanan pada sistem informasi akademik kampus. Melalui metode pengujian penetrasi (*penetration testing*), OWASP ZAP memindai aplikasi *web* dan berhasil mengidentifikasi berbagai celah keamanan yang dikategorikan sesuai standar OWASP Top 10. Hasil penelitian menunjukkan bahwa ZAP mampu mendeteksi kerentanan pada berbagai tingkatan risiko. Tahapan penggunaan ZAP meliputi perencanaan, pemindaian celah keamanan menggunakan metode *automated scanning* dan *intercepting proxy*, eksploitasi celah (*gaining access*), serta analisis hasil temuan. Dengan penerapan OWASP ZAP organisasi dapat melakukan evaluasi mandiri terhadap keamanan aplikasinya, sehingga mampu mengambil langkah mitigasi yang tepat sesuai dengan kerentanan yang ditemukan.

Tabel 1. Penelitian - Penelitian Terkait

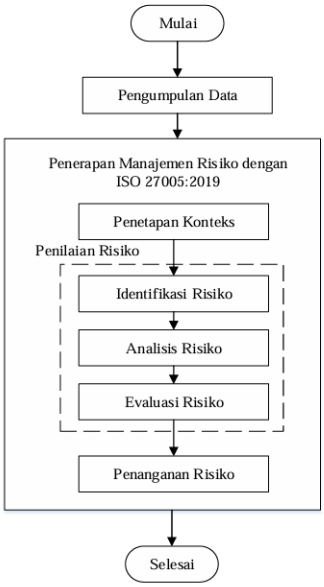
Peneliti	Objek	Metode	Hasil	Langkah Selanjutnya
Utami, G.C. dkk. [9]	Website IITC Intermedia (Univ. Amikom)	ISO 27005:2018 + DREAD	Risiko *availability* tertinggi saat *upload*; nilai risiko *sedang* (rata-rata 11,5); rekomendasi: *asset- & tool-based risk assessment*	Melakukan rekomendasi peningkatan mitigasi teknis berbasis peringkat risiko
Jonny, J. dkk [10]	Sistem Informasi Puskesmas (SIMPUS)	ISO/IEC 27005	Mengidentifikasi 30 skenario ancaman (DDoS, pengaksesan ilegal, kebocoran data pasien).	Menyusun strategi *Risk Modification* dan kontrol teknis seperti *firewall*, *backup system*, dan *log* akses.
Ashari, I. F., dkk. [11]	Website E-learning ITERA	OWASP ZAP active scan	9 kerentanan, termasuk SQL *Injection* dan CSRF; 3 URI berisiko tinggi	Penerapan *filter input*, *control heade*r, dan mitigasi *brute-force.*
Ramadhan, M.F., Ilamananda, A.S. [8]	SIAKAD Universitas Merdeka Malang	OWASP ZAP scan	17 celah (3 *high*, 3 *medium*, 5 *low*, 6 info); XSS, *injection*, *misconfig*	Rekomendasi berdasarkan OWASP A02–A05, *training* tim IT

Secara umum, temuan dari Tabel 1 menunjukkan bahwa meskipun metode ISO/IEC 27005 dan OWASP ZAP telah diterapkan secara luas dalam menganalisis risiko dan mengidentifikasi kerentanan pada berbagai sistem informasi, belum ditemukan penelitian yang secara **t**erintegrasi menggabungkan keduanya dalam konteks pelayanan publik *e-commerce* seperti *website* Peken Surabaya. Penelitian ini hadir untuk mengisi kekosongan tersebut dengan menggabungkan analisis risiko berbasis ISO/IEC 27005:2019 dan hasil pemindaian teknis

menggunakan OWASP ZAP pada sistem *website* Peken Surabaya guna memberikan pemetaan risiko yang sistematis tetapi juga validasi teknis terhadap potensi celah keamanan yang nyata dan aplikatif dalam meningkatkan keamanan siber sistem pelayanan publik digital.

3. METODE PENELITIAN

Proses analisis risiko keamanan informasi pada *website* Peken Surabaya dalam penelitian ini dilakukan dengan 2 tahapan yaitu berdasarkan standar manajemen risiko informasi ISO/IEC 27005:2019 dan pengujian teknis dengan *tool* OWASP ZAP. *Framework* ISO 27005:2019 digunakan karena merupakan standar internasional dimana framework tersebut menyediakan pedoman dalam manajemen risiko keamanan informasi di dalam sebuah instansi atau organisasi [10]. Langkah-langkah dalam proses analisis ini disusun mengikuti kerangka kerja ISO 27005:2019 dan dijelaskan secara terstruktur dalam Gambar berikut:



Gambar 1. Tahapan analisis risiko

Tahap pertama adalah analisis risiko menggunakan standar ISO/IEC 27005:2019. Penelitian ini diawali dengan tahap pengumpulan data melalui wawancara dan studi pustaka. Observasi dilakukan terhadap pengguna website, sedangkan studi pustaka dilakukan dengan menelaah berbagai literatur, khususnya melalui review jurnal. Selanjutnya dilakukan identifikasi aset penting dalam sistem *website* Peken Surabaya, seperti *database* UMKM, data pengguna, dan modul transaksi. Selanjutnya, identifikasi potensi ancaman dan kerentanan yang mungkin terjadi terhadap aset tersebut, dilanjutkan dengan analisis risiko menggunakan matriks yang mengukur tingkat dampak dan kemungkinan kejadian. Evaluasi dilakukan untuk

menentukan risiko mana yang perlu ditangani, lalu dirumuskan strategi mitigasi sesuai tingkat urgensinya.

Gambar 2. Tahapan *Intercepting proxy*

Tahap kedua dalam penelitian ini merupakan pengujian teknis menggunakan OWASP ZAP (*Zed Attack Proxy*) melalui proses pemindaian otomatis untuk mendeteksi kerentanan umum seperti *SQL Injection*, *Cross-Site Scripting* (XSS), *security misconfiguration*, dan *broken authentication*. Sistem *website* Peken Surabaya diuji secara langsung oleh ZAP, kemudian hasilnya dianalisis berdasarkan panduan OWASP Top 10, yaitu daftar sepuluh jenis celah keamanan paling umum dalam aplikasi *web* [9]. Temuan ini digunakan untuk memverifikasi kerentanan aktual dalam sistem dan memperkuat hasil analisis risiko pada tahap sebelumnya. Kemudian rekomendasi pengendalian disusun sebagai hasil kombinasi antara pendekatan manajerial berbasis ISO/IEC 27005:2019 dan temuan teknis berbasis praktik terbaik dari OWASP ZAP.

4. HASIL DAN PEMBAHASAN

Penelitian ini menggunakan standar ISO/IEC 27005:2019 sebagai kerangka dalam mengelola risiko keamanan informasi pada *website* Peken Surabaya milik Pemerintah Kota Surabaya. Platform *website* Peken Surabaya merupakan layanan berbasis *e-commerce* yang bertujuan untuk memberdayakan pelaku UMKM lokal. Oleh karena itu, sistem ini memiliki peran krusial dan menyimpan data penting yang perlu dilindungi dari ancaman siber. Analisis risiko dilakukan melalui beberapa tahapan, dimulai dari penetapan konteks, identifikasi aset, identifikasi ancaman dan kerentanan, penilaian risiko, hingga penanganan risiko. Selain itu, dilakukan juga pengujian teknis menggunakan OWASP ZAP guna mendeteksi kerentanan aktual pada sistem *website* Peken Surabaya.

TAHAP 1: ISO/IEC 27005:2019

1. Penetapan Konteks

Tahapan awal dalam manajemen risiko yang diterapkan dalam penelitian ini mengacu pada standar ISO 27005:2019, yang dimulai dengan penetapan konteks. Pada tahap ini, ruang

lingkup analisis difokuskan pada *website* Peken Surabaya sebagai salah satu platform mengakselerasi potensi UMKM setempat yang dirilis oleh Pemkot Surabaya.

2. Penilaian Risiko

Penilaian risiko pada *website* Peken Surabaya dilakukan melalui tiga tahap utama: identifikasi, analisis, dan evaluasi risiko.

2.1 Identifikasi Risiko

Identifikasi risiko terdiri dari beberapa proses diantaranya identifikasi aset, identifikasi ancaman, identifikasi *existing control* & identifikasi *vulnerabilities*. Identifikasi risiko keamanan informasi pada *website* Peken Surabaya dilakukan untuk mengetahui potensi ancaman terhadap aset-aset penting yang terlibat dalam operasionalnya. Ancaman terhadap aset teknologi informasi (TI) pada *website* Peken Surabaya dapat berasal dari berbagai faktor, termasuk serangan siber, kesalahan pengguna (*human error*), maupun gangguan teknis lainnya. Berikut rincian identifikasi ancaman ini disajikan dalam Tabel 2.

Tabel 2. Identifikasi Ancaman *Website* Peken Surabaya

No	Aset	Kode Aset	Ancaman
1	Infrastruktur TI (Server & Jaringan)	I1	Serangan DDoS yang membuat sistem tidak bisa diakses saat *traffic* tinggi (*flash sale*, promo UMKM)
		I2	Gangguan *server* seperti *overload*, *misconfiguration*, atau pemadaman mendadak
		I3	Jaringan lambat atau tidak stabil menyebabkan kegagalan saat *checkout*/pembayaran
2	Aplikasi (*Web* & *Backend*)	A1	*Bug* sistem menyebabkan order ganda, keranjang tidak tersimpan, atau data pembayaran hilang
		A2	*API abuse* atau akses tidak sah melalui endpoint produk, transaksi, atau akun
		A3	*Phishing login* terhadap pelapak atau pembeli melalui link palsu mirip *Website* Peken
		A4	Penyalahgunaan session token (misal sesi tidak *expired* otomatis, atau digunakan lintas perangkat)
3	Data Pengguna & UMKM	D1	Kebocoran data pelapak atau pembeli (alamat, no HP, nama toko, data rekening, dsb.)
		D2	Pengambilalihan akun pelapak / pembeli oleh pihak tidak sah *(account takeover)*
		D3	Penyalahgunaan data produk oleh pihak eksternal (*copy* produk massal, *scraping* gambar/deskripsi)
4	Sistem Transaksi & Pembayaran	T1	Transaksi palsu / gagal akibat *bug* saat proses pembayaran
		T2	Pemalsuan bukti pembayaran oleh pembeli, atau manipulasi nominal oleh pelapak
		T3	Data transaksi tidak terenkripsi atau terekam secara tidak aman dalam server
5	Pengguna	U1	*Human error* saat input produk (harga salah, gambar tidak relevan) atau saat *checkout*
		U2	Rendahnya kesadaran keamanan pengguna (klik

		tautan *phising*, tidak logout di perangkat umum)
	U3	Akun tidak menggunakan autentikasi ganda (tidak ada OTP/email verifikasi login)

Tabel 2 di atas menjelaskan berbagai ancaman keamanan yang berpotensi terjadi pada sistem dan pengguna *website* Peken Surabaya. Ancaman ini meliputi aspek infrastruktur, *website*, data pengguna, sistem transaksi, dan pengguna.

Selanjutnya dilakukan proses identifikasi *existing control* yang bertujuan untuk mengenali pengendalian yang telah diterapkan pada aset, sehingga dapat mencegah pengeluaran biaya yang tidak perlu. Sedangkan identifikasi *vulnerabilities* menggambarkan adanya kelemahan yang mungkin dimanfaatkan dan dapat berdampak pada aset yang dimiliki [12]. Berikut adalah hasil identifikasi *existing control* dan *vulnerabilities* pada aset-aset penting yang dimiliki oleh sistem *website* Peken Surabaya disajikan dalam Tabel 3.

Tabel 3. Identifikasi *existing control* dan *vulnerabilities* pada *Website* Peken Surabaya

Nama Asset	***Existing controls* (Kontrol yang ada)**	***Vulnerabilities* (Kerentanan)**
Infrastruktur TI (Server & Jaringan)	Penggunaan *firewall*, WAF, dan SSL /TLS untuk mengenkripsi koneksi	Tidak semua *endpoint* menggunakan WAF
	Load balancing saat trafik tinggi	Layanan tidak dapat menangani trafik lonjakan
	Backup data rutin	Potensi kegagalan *backup* atau pemulihan sistem lambat
Aplikasi (*Web* & *Backend*)	Enkripsi data transaksi & autentikasi	*Bug* dalam logika pemrosesan *order*
	Logging aktivitas pengguna	Tidak ada *session timeout* otomatis
	Validasi *input* pada *form* & halaman *checkout*	Beberapa *form* masih rawan *XSS / SQL injection*
Data Pengguna (Pembeli dan Pelapak)	*Form login* terenkripsi dengan HTTPS	Data pribadi rentan jika *database* tidak terenkripsi
	Penggunaan *username* dan *password* unik	Akun rawan diambil alih karena *password reuse* atau lemah
	Kebijakan privasi pengguna terpublikasi	Tidak adanya 2FA untuk pelapak maupun admin
Sistem Transaksi & Pembayaran	Integrasi *gateway* pembayaran dengan OTP	Tidak semua transaksi menggunakan verifikasi dua langkah
	Validasi data transaksi sebelum konfirmasi	Pemalsuan bukti bayar oleh pengguna sulit diverifikasi otomatis
	Pencatatan historis transaksi	Transaksi gagal karena *bug* tidak terdeteksi *real-time*
Pengguna	Verifikasi email saat registrasi	Rendahnya kesadaran keamanan pengguna
	Panduan penggunaan di FAQ & edukasi dasar di media sosial	*Phishing link* mudah disebar melalui WA, komentar produk, dsb.

Tabel 3 menunjukkan pengendalian keamanan yang telah diterapkan pada aset utama *website* Peken Surabaya beserta kerentanannya. Pada infrastruktur TI, meskipun telah

menggunakan *firewall, WAF,* dan *SSL*, masih terdapat celah dalam menangani lonjakan trafik saat promo. Di sisi aplikasi, enkripsi dan validasi form sudah diterapkan, namun masih ditemukan *bug* pada sistem order serta celah *XSS* dan *SQL injection.* Data pengguna telah dilindungi dengan *HTTPS* dan *password* unik, tetapi *reuse password* dan data yang belum terenkripsi tetap menjadi risiko. Sistem transaksi telah dilengkapi OTP dan validasi, namun verifikasi dua langkah belum optimal dan potensi pemalsuan bukti bayar masih ada. Sementara itu, rendahnya edukasi keamanan pengguna meningkatkan risiko penyalahgunaan. Daftar ini menjadi dasar analisis risiko untuk menilai kemungkinan dan dampak dari setiap kerentanan terhadap *website*.

2.2 Analisis Risiko

Berdasarkan hasil identifikasi pada tabel 3, dilakukan proses penilaian dari masing-masing risiko. Penilaian diberikan dengan mengacu pada kemungkinan ancaman serta dampak dari terjadinya sebuah risiko. Kategori penilaian ancaman dibagi menjadi 5, yaitu *very unlikely* (1), *unlikely* (2), *possible* (3), *likely* (4), dan *frequent* (5). Sedangkan kategori penilaian dampak dibagi menjadi 5, yaitu *very low* (1), *low* (2), *medium* (3), *high* (4), *very high* (5). Tabel 3 dibawah ini memuat hasil penilaian risiko yang didasarkan pada nilai ancaman serta nilai dampak untuk seluruh aset. Setiap aset ditandai dengan kode tertentu seperti I untuk Infrastruktur TI, A untuk Aplikasi, D untuk Data Pengguna, T untuk Sistem Transaksi, dan U untuk Pengguna.

Tabel 4. Analisis Risiko pada *Website* Peken Surabaya

Nama Asset	**Kode**	***Existing controls* (Kontrol yang ada)**	***Vulnerabilities* (Kerentanan)**	**Nilai Ancaman**	**Nilai Dampak**
Infrastruktur TI (Server & Jaringan)	I1	*Load balancer*, CDN	Kapasitas tidak bisa menahan lonjakan traffic	*Frequent*	*Very High*
	I2	*Backup server, disaster recovery plan*	Belum ada sistem pemulihan cepat otomatis	*Likely*	High
	I3	Monitoring jaringan dasar	Tidak ada *auto failover* jaringan	*Likely*	*High*
Aplikasi *(Web & Backend)*	A1	QA *testing manual*	Kurangnya *regression test*	*Likely*	*High*
	A2	*Token access control*	*Endpoint* tidak dilindungi autentikasi kuat	*Frequent*	*Very High*
	A3	Email resmi, notifikasi	Tidak ada *domain warning* atau proteksi *link* eksternal	*Possible*	Medium
	A4	*Session management*	*Session* tidak kadaluarsa otomatis / *multi-device*	*Unlikely*	*Low*

Data Pengguna (Pembeli dan Pelaku Usaha)	D1	Enkripsi dasar & *login password*	Data disimpan *plaintext*/*log serve*r tidak aman	*Frequent*	*Very High*
	D2	*Login password*, OTP	Tidak semua akun memakai OTP/email verifikasi	*Frequent*	*Very Hugh*
	D3	CAPTCHA, *login* untuk akses produk	Gambar/deskripsi produk bebas diakses publik	*Unlikely*	*Low*
Sistem Transaksi & Pembayaran	T1	Validasi *backend*	Kurangny*a error handling & log* transaksi *real-time*	*Likely*	*High*
	T2	*Upload* manual bukti bayar	Tidak ada verifikasi sistem (hash/timestamp)	*Possible*	*Medium*
	T3	*Database basic secured*	Tidak semua data ditransmisikan via HTTPS	*Likely*	*High*
Pengguna	U1	*Form validation*	Tidak semua *field divalidasi* otomatis	*Possible*	*Medium*
	U2	Edukasi email/notifikasi	Tidak ada pelatihan atau notifikasi risiko login	*Unlikely*	*Low*
	U3	*Login password*	Tidak ada OTP/2FA/email verifikasi *login*	*Likely*	*High*

Tabel 4 analisis risiko memuat penilaian untuk masing-masing ancaman serta dampak secara kualitatif. Penilaian kualitatif dilakukan dengan mengartikan ancaman dan risiko ke dalam kategori yang telah ditentukan sebelumnya. Setelahnya dilanjutkan dengan penilaian kuantitatif dengan hasil yang dapat dilihat pada tabel 5.

Tabel 5. Hasil Penilaian Level Risiko pada *Website* Peken Surabaya

Kode	Nilai Ancaman	Nilai Dampak	Nilai Risiko	Level Risiko
I1	5	5	25	*High*
I2	4	4	16	*High*
I3	3	4	12	*Medium*
A1	4	4	16	*High*
A2	5	5	25	*High*
A3	3	4	12	*Medium*
A4	1	4	4	*Low*
D1	5	5	25	*High*
D2	5	5	25	*High*
D3	1	3	3	*Low*
T1	4	4	16	*High*
T2	2	4	8	*Medium*
T3	4	5	20	*High*
U1	3	3	9	*Medium*
U2	2	2	4	*Low*
U3	5	5	25	*High*

Tabel 5 berisi hasil penilaian level risiko yang diidentifikasi dari berbagai potensi ancaman terhadap sistem dan operasional *website* Peken Surabaya. Penilaian dilakukan dengan

mengalikan nilai ancaman (kemungkinan terjadinya suatu kejadian) dengan nilai dampak (tingkat kerugian atau gangguan yang ditimbulkan) [12]. Nilai ancaman dan nilai dampak masing-masing diberi skor antara 1 (terendah) hingga 5 (tertinggi), sehingga nilai risiko total berkisar antara 1 hingga 25. Berdasarkan nilai risiko tersebut, risiko dikategorikan ke dalam tiga level, yaitu: *Low* (rendah) untuk nilai risiko 1–4, *Medium* (sedang) untuk nilai 5–14, dan *High* (tinggi) untuk nilai 15–25.

Dalam tabel 5 menunjukkan bahwa sebagian besar risiko pada *website* Peken Surabaya berada pada kategori *Very High* dan *High*, menandakan ancaman serius terhadap keamanan dan ketersediaan sistem. Risiko seperti serangan DDoS (I1), kebocoran data pengguna (D1, D2), dan tidak adanya fitur 2FA (U3) termasuk dalam kategori *Very High* karena dampak dan ancamannya tinggi, sehingga perlu penanganan segera. Risiko dalam kategori *High* seperti gangguan server (I2), serangan pada aplikasi (A1), dan gangguan transaksi (T1, T3) juga perlu prioritas pengendalian. Risiko *Medium* seperti gangguan jaringan (I3) dan *human error* (U1) tetap memerlukan pengawasan untuk mencegah eskalasi. Risiko *Low* seperti kelemahan minor (A4, U2, D3) tetap perlu dipantau sebagai langkah pencegahan. Secara keseluruhan, hasil penilaian risiko ini menjadi dasar penting untuk menentukan prioritas penanganan keamanan siber di *website* Peken Surabaya selanjutnya.

2.3 Evaluasi Risiko

Tabel 6. Matriks Penilaian Risiko pada *Website* Peken Surabaya

Dampak	Kemungkinan Terjadinya Ancaman (1)	(2)	(3)	(4)	(5)
(1)					
(2)					
(3)	D3		U1	I3, A3	
(4)	A4	T2		I2, A1, T1, U2	
(5)			T3		I1, A2, D1, D2, U3

Tabel 6 menggambarkan *Matriks Penilaian Risiko* yang menyajikan hubungan antara kemungkinan terjadinya ancaman (nilai ancaman) dan tingkat dampak yang ditimbulkan. Matriks ini dibagi menjadi tiga kategori warna berdasarkan tingkat risiko: hijau untuk risiko rendah (*low*), kuning untuk risiko sedang (*medium*), dan merah untuk risiko tinggi (*high*). Dengan demikian, jika dilihat dari warna, tabel di atas menunjukkan bahwa hasil rata-rata risiko tinggi. Penempatan kode aset matriks menunjukkan posisi masing-masing risiko berdasarkan hasil evaluasi nilai ancaman dan dampaknya.

Tabel 7. Daftar Level Risiko yang mungkin terjadi pada *Website* Peken Surabaya

Level Risiko	Kode Aset
Low (L)	D3, A4
Medium (M)	U1, T2, I3, A3
High (H)	I1, I2, A1, A2, D1, D2, T1, T3, U2, U3

Tabel 7 pengelompokan aset berdasarkan tingkat resikonya. Mayoritas aset termasuk dalam kategori risiko tinggi (*high*). Artinya, aspek tersebut memerlukan pengendalian dan pemantauan yang lebih serius. Klasifikasi ini membantu menentukan prioritas pengelolaan risiko dalam organisasi.

2.4 Penanganan Risiko

Setelah tahap penilaian risiko, dilakukan pemilihan tindakan untuk menangani risiko dengan empat jenis perlakuan sesuai dengan standar, yaitu modifikasi risiko (*Risk Modification*/RM), mempertahankan risiko (*Risk Retention*/RR), menghindari risiko (*Risk Avoidance*/RA), dan membagi risiko (Risk *Sharing*/RS). Hasil dari penilaian ini ditampilkan dalam Tabel 8.

Tabel 8. Hasil Penilaian Risiko pada *Website* Peken Surabaya

Kode	Level Risiko	Biaya Pemulihan	Penanganan Risiko	Keterangan
I1	*Very High*	*High*	RM	Penguatan *firewall* dan WAF (Perlindungan *Traffic*)
I2	*High*	*Medium*	RM	Peningkatan *disaster recovery*
I3	*Medium*	*Medium*	RM	Evaluasi penyedia *cloud* & SLA
A1	*High*	*Medium*	RS	Peningkatan *logging* dan sesi
A2	*Very High*	*High*	RM	Perbaikan proses QA dan *rollback system*
A3	*Medium*	*Low*	RA	Proses verifikasi ganda & pembatasan sesi bagi *user*
A4	*Low*	*Low*	RR	*Update* token berkala & *session security*
D1	*Very High*	*High*	RM	Pengamanan akses pihak ketiga & enkripsi *database*
D2	*Very High*	*Medium*	RM	Sistem pendeteksi *anomaly login* & OTP *Protection*
D3	*Low*	*Low*	RA	Edukasi pengguna untuk menjaga privasi dalam bertransaksi
T1	*High*	*Medium*	RM	Peningkatan validasi transaksi
T2	*Medium*	*Medium*	RM	Peningkatan integritas bukti transaksi & *audit trail*
T3	*High*	*Medium*	RM	Transparansi data dalam melacak status pesanan
U1	*Medium*	*Low*	RA	Edukasi untuk mengkonfirmasi tindakan sebelum dieksekusi
U2	*Low*	*Low*	RR	Penyuluhan *Digital Security* &

				simulasi terhadap risiko
U3	*Very High*	*Low*	RR	Dorongan aktivasi wajib 2FA & verifikasi perangkat

Dari Tabel 8, hasil penanganan risiko pada *website* Peken Surabaya menunjukkan bahwa sebagian besar risiko ditangani menggunakan pendekatan *Risk Modification* (RM), yaitu dengan melakukan pengendalian untuk menurunkan kemungkinan terjadinya atau dampak dari risiko. Pendekatan RM diterapkan pada risiko dengan tingkat risiko *Medium* hingga *Very Hig*h dan biaya pemulihan yang *Medium* hingga *High*, seperti pada I1, I2, I3, A2, D1, D2, T1, T2, T3, U1, dan U3. Contohnya adalah penerapan enkripsi *database*, penguatan *firewall*, peningkatan *disaster recovery*, serta sistem deteksi anomali login dan audit *trail* transaksi.

Tabel ini juga menunjukkan penggunaan pendekatan *Risk Retention* (RR) pada risiko dengan dampak rendah atau biaya pemulihan minimal, seperti A4, U2, dan U3, yang ditangani melalui langkah preventif seperti pembaruan token, penyuluhan keamanan digital, dan dorongan aktivasi 2FA. Sementara itu, pendekatan *Risk Avoidance* (RA) digunakan pada risiko dengan melalui perubahan proses atau perilaku pengguna, seperti pada A3, D3, dan U1, melalui verifikasi ganda, edukasi privasi, dan konfirmasi tindakan. Ada pula satu risiko (A1) yang ditangani melalui *Risk Sharing* (RS), yaitu dengan meningkatkan *logging* dan pengelolaan sesi, yang dapat dibantu oleh pihak ketiga atau layanan penyedia eksternal.

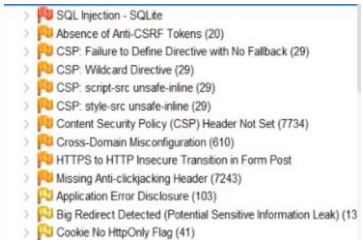
Berdasarkan hasil analisis penilaian risiko yang terdapat pada Tabel 8, maka rekomendasi yang tepat untuk penanganan risiko keamanan informasi berdasarkan standar ISO/IEC 27005:2019 adalah sebagai berikut:

1. **Kode kontrol rekomendasi untuk I1 dan I2** yaitu *Protection from physical and environmental threats* (A.8.23, A.8.20) dengan menerapkan sistem perlindungan terhadap gangguan fisik seperti serangan DDoS melalui WAF/CDN serta sistem redundansi dan pemulihan bencana.
2. **Kode kontrol rekomendasi untuk I3** yaitu *Monitoring and logging* (A.8.16, A.8.22) dengan melakukan pemantauan lalu lintas jaringan dan aktivitas *cloud* secara *real-time* untuk mendeteksi risiko eksternal.
3. **Kode kontrol rekomendasi untuk A1 dan A4** yaitu *Secure development life cycle, and web application security* (A.8.9, A.8.25) dengan menerapkan pengelolaan sesi seperti *logout* otomatis dan *rollback* pada perubahan aplikasi.
4. **Kode kontrol rekomendasi untuk A2 dan A3** yaitu *Protection against malicious code and secure coding* (A.8.24, A.8.28) dengan memperkuat mekanisme validasi API, dan penggunaan OTP ganda.

5. **Kode kontrol rekomendasi untuk D1 dan D3** yaitu *Cryptographic controls and protection of PII* (A.8.12, A.8.32) dengan melakukan enkripsi menyeluruh pada database pengguna dan retensi data diminimalisir.
6. **Kode kontrol rekomendasi untuk D2 dan U2** yaitu *Information security awareness and identity management* (A.6.3, A.8.30) dengan memberikan edukasi keamanan terhadap pengguna, termasuk kampanye *anti-phishing* dan keamanan data pribadi.
7. **Kode kontrol rekomendasi untuk T1 dan T3** yaitu *Information backup and auditing* (A.8.14, A.8.31) melalui backup berkala serta pendeteksi kesalahan total belanja & pengembalian dana.
8. **Kode kontrol rekomendasi untuk T2** yaitu *Transaction validation* (A.13.2.4) melalui penerapan validasi transaksi yang ketat menggunakan OTP/PIN dan sistem deteksi anomali otomatis.
9. **Kode kontrol rekomendasi untuk U1** yait*u Terms & conditions of employment & awareness* (A.6.2, A.6.3) dengan konfirmasi tindakan melalui *pop-up*.
10. **Kode kontrol rekomendasi untuk U3** yait*u Identity management & access control* (A.9.30, A.8.21) dengan konfirmasi aktivitas melalui penggunaan 2FA.

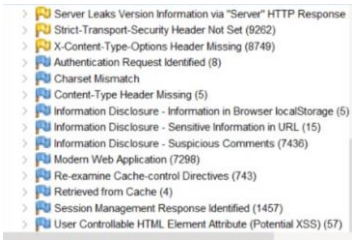
TAHAP 2: OWASP ZAP

Setelah dilakukan analisis risiko menggunakan standar ISO/IEC 27005:2019, didapatkan identifikasi dan penilaian terhadap tingkat risiko dari berbagai ancaman yang mungkin terjadi pada *website* Peken Surabaya. Analisis ini menjadi dasar dalam menentukan prioritas pengendalian keamanan informasi. Selanjutnya, untuk memperkuat hasil analisis tersebut, pengujian teknis dilakukan menggunakan *tools* dari OWASP (*Open Web Application Security Project)* guna mendeteksi kerentanan secara langsung pada *website* Peken Surabaya.



Gambar 3. Owasp Zap 1

Gambar 4. Owasp Zap 2



Gambar 5. Owasp Zap 2

OWASP ZAP yang ditampilkan pada Gambar 3 dan Gambar 4, *website* Peken Surabaya mengandung beberapa kerentanan yang berpotensi membahayakan keamanan informasi pengguna. Pada Gambar 3, ditemukan kerentanan kritikal seperti SQL *Injection* pada *database SQLite* yang memungkinkan penyerang mengeksekusi perintah berbahaya pada *database*. Selain itu, tidak adanya *Anti-CSRF* token membuka peluang terjadinya serangan permintaan

lintas situs. Masalah *Content Security Policy (CSP)* seperti penggunaan *wildcard directive, unsafe-inline script/style*, dan *header* CSP yang tidak disetel, berpotensi menyebabkan serangan *Cross-Site Scripting* (XSS). Kerentanan lain termasuk *Cross-Domain Misconfiguration*, transisi HTTP tidak aman, dan tidak adanya *header anti-clickjacking*.

Sementara itu, pada Gambar 4, kerentanan berfokus pada konfigurasi *header* keamanan yang lemah dan pengungkapan informasi sensitif. Beberapa temuan mencakup tidak adanya *flag Secure* dan *HttpOnly* pada *cookie*, ketidakhadiran *header* penting seperti *Strict-Transport-Security* dan *X-Content-Type-Options*, serta pengungkapan versi *server* yang bisa dimanfaatkan penyerang untuk menemukan celah. Selain itu, ditemukan pula informasi sensitif yang tersimpan di URL, *local Storage*, dan pesan *error debug*. Beberapa temuan menunjukkan adanya inkonsistensi otentikasi, kesalahan konten, dan potensi injeksi HTML melalui atribut input pengguna.

Tabel 9. Klasifikasi kerentanan berdasarkan OWASP TOP 10

Kode	Vulnerabilities	Alerts	Level Risiko
A01	*Broken Access Control*	*Absence of Anti-CSRF Tokens*	*Medium*
A02	*Cryptographic Failures*	*Cookie No HttpOnly Flag* *Cookie Without SameSite Attribute* *Secure Pages Include Mixed Content*	*Low*
A03	*Injection*	*Cross-Site Scripting (Reflected)* *SQL Injection* *SQL Injection – SQLite*	*High*
A04	*Insecure Design*	*Vulnerable JS Library*	*Medium*
A05	*Security Misconfiguration*	*Content Security Policy (CSP) Header Not Set* *CSP Wildcard / unsafe-inline Directives* *Missing Anti-Clickjacking Header* *X-Content-Type-Options Header Missing*	*Medium*
A06	*Vulnerable and Outdated Components*	*Modern Web Application (general component exposure)*	*Informational*
A07	*Identification and Authentication Failures*	*Authentication Requests Identified* *User Agent Fuzzer*	*Informational*
A08	*Software and Data Integrity Failures*	*Session Management Response Identified*	*Informational*
A09	*Security Logging and Monitoring Failures*	*Information Disclosure – Debug Error Messages*	*Informational*

A10	*Server-Side Request Forgery*	*Cross-Domain JavaScript Source File Inclusion*	*Informational*

Berdasarkan Tabel 9, ditemukan sebanyak 15 kerentanan pada hasil analisis keamanan *website* Peken Surabaya. Distribusi tingkat risiko dari kerentanan tersebut adalah sebagai berikut: *High Risk Level* sebesar 20% atau 3 kerentanan, *Medium Risk Level* sebesar 26,67% atau 4 kerentanan, *Low Risk Level* sebesar 20% atau 3 kerentanan, dan *Informational Risk Level* sebesar 33,33% atau 5 kerentanan. Selanjutnya, hasil pengujian kerentanan yang mengacu pada pedoman OWASP Top 10 dijadikan dasar dalam penyusunan rekomendasi penanganan risiko. Rekomendasi untuk kerentanan dengan tingkat risiko tinggi (*High*) dan sedang (*Medium*) dapat dilihat pada Tabel 10.

Tabel 10. Rekomendasi Pengendalian Kerentanan berdasarkan OWASP TOP 10.

Vulnerabilities	**Rekomendasi**
A01 - *Broken Access Contro*l	- Menerapkan akses berdasarkan peran pengguna. - Menerapkan validasi pada setiap aksi. - Memantau aktivitas pengguna.
A03 - *Injection*	- Menggunakan *parameterized queries*. - Menerapkan validasi pada proses input. - Menggunakan ORM untuk mengurangi akses SQL secara langsung.
A04 - *Insecure Design*	- Menerapkan keamanan pada setiap desain. - Menjalankan *threat modeling* pada tahap pengembangan. - Menggunakan *library* yang terjamin.
A05 - *Security Misconfiguration*	- Konfigurasi *header* keamanan: CSP, X-*Frame-Options*, X-*Content-Type-Options*. - Mematikan informasi debug di lingkungan produksi. - Menerapkan konfigurasi minimum *exposure*.

Secara keseluruhan, temuan-temuan ini menunjukkan bahwa *website* Peken Surabaya masih memerlukan perbaikan signifikan dalam aspek konfigurasi keamanan, proteksi data pengguna, dan penerapan *best practice* pengembangan *website* yang aman sesuai dengan standar OWASP dan ISO/IEC 27005:2019.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian keamanan terhadap *website* Peken Surabaya dilakukan melalui pendekatan analisis risiko berdasarkan standar ISO/IEC 27005:2019, dilanjutkan dengan pengujian teknis menggunakan pedoman OWASP Top 10, dapat disimpulkan bahwa sistem masih memiliki sejumlah kerentanan yang signifikan. Hasil laporan *scanning* OWASP ZAP menunjukkan adanya 15 kerentanan dengan distribusi risiko sebanyak 3 kerentanan

berkategori *High* (20%), 4 *Medium* (26,67%), 3 *Low* (20%), dan 5 *Informational* (33,33%). Risiko dengan tingkat *Very High* dan *High* seperti serangan DDoS, kebocoran data pengguna, serta tidak adanya sistem autentikasi dua faktor, berpotensi besar mengganggu kerahasiaan, integritas, dan ketersediaan layanan. Rekomendasi kontrol keamanan yang sesuai telah ditetapkan berdasarkan ISO/IEC 27005:2019, termasuk proteksi fisik dan lingkungan, enkripsi data, serta penguatan manajemen identitas. Selain itu, hasil pengujian kerentanan berdasarkan OWASP mengindikasikan masih adanya celah pada aspek *Broken Access Control, Injection, Insecure Design,* dan *Security Misconfiguration* yang membutuhkan penanganan segera.

Berdasarkan hasil tersebut, disarankan agar pengelola *website* Peken Surabaya memprioritaskan penanganan kerentanan dengan tingkat risiko *High* dan *Medium*. Langkah awal mencakup penerapan *WAF/CDN* untuk mitigasi DDoS, aktivasi *2FA/OTP*, enkripsi data pengguna, serta penerapan prinsip *secure coding* dan konfigurasi keamanan yang tepat. Selain itu, pemantauan *real-time, backup* berkala, dan edukasi keamanan juga perlu dilakukan untuk membangun pertahanan menyeluruh. Rekomendasi lebih rinci telah dijelaskan pada bagian penanganan risiko melalui pemberian kode kontrol sesuai ISO/IEC 27005:2019 dan pada Tabel 10 yang memuat solusi berdasarkan kerentanan *High* dan *Medium* sesuai pedoman OWASP Top 10. Implementasi menyeluruh dari rekomendasi tersebut diharapkan dapat meningkatkan keamanan serta kepatuhan terhadap standar keamanan informasi *website* Peken Surabaya secara berkelanjutan.

DAFTAR REFERENSI

Akbhari, I., & Prathama, A. (2023). Inovasi aplikasi E-Peken: Optimalisasi potensi UMKM Kota Surabaya. *NeoRespublica: Jurnal Ilmu Pemerintahan, 4*(2), 396–409. https://doi.org/10.52423/neoresjurnal.v4i2.90

Ardius, E., & Syamsuar, D. (2023). Assessment risk terhadap penggunaan sistem informasi akademik Universitas Ea menggunakan metode ISO 27001. *Jurnal Teknologi Informasi Mura, 15*(1), 1–13. https://doi.org/10.32767/jti.v15i1.1948

Aryani, F. D., Hastuti, A. K., Rohmawati, W., Kasiwi, A. N., & Winarsih, A. S. (2021). Inovasi E-Lampid sebagai implementasi New Public Service dalam meningkatkan kualitas pelayanan Disdukcapil Kota Surabaya. *NeoRespublica: Jurnal Ilmu Pemerintahan, 2*(2), 178. http://dx.doi.org/10.52423/neores.v2i2.17654

Isnaini, K., Sari, G. J. N., & Kuncoro, A. P. (2023). Analisis risiko keamanan informasi menggunakan ISO 27005:2019 pada aplikasi sistem pelayanan desa. *Jurnal Eksplora Informatika, 13*(1), 37–45. https://doi.org/10.30864/eksplora.v13i1.696

Jonny, J., Ambarwati, A., & Darujati, C. (2021). Penilaian risiko data sistem informasi manajemen puskesmas dan aset menggunakan ISO 27005. *SISTEMASI, 10*(1), 1. https://doi.org/10.32520/stmsi.v10i1.995

Leasa, Z. V., & Prassida, G. F. (2024). Manajemen risiko pada sistem informasi akademik Universitas XYZ menggunakan ISO 27005:2018. *Jurnal Teknologi dan Sistem Informasi Bisnis, 6*(4), 649–656. https://doi.org/10.47233/jteksis.v6i4.1459

Ramadhan, D. L., Febriansyah, R., & Dewi, R. S. (2020). Analisis manajemen risiko menggunakan ISO 31000 pada smart canteen SMA XYZ. *JURIKOM (Jurnal Riset Komputer), 7*(1), 91. https://doi.org/10.30865/jurikom.v7i1.1791

Ramadhan, M. F. A., & Ilmananda, A. S. (2024). Analisis ancaman keamanan pada sistem informasi akademik kampus menggunakan metode OWASP ZAP. *JATI (Jurnal Mahasiswa Teknik Informatika), 8*(4), 7985–7991. https://doi.org/10.36040/jati.v8i4.10599

Rambe, R., Gandhi, A., & Sabariah, M. K. (2023). Implementasi manajemen risiko pada aplikasi XYZ dengan pendekatan SNI ISO/IEC 27005:2018. *eProceedings of Engineering, 10*(4). https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/20846

Sati, D. L., Sita, D. L., & Isnaini, K. N. (2024). Identifikasi celah kerentanan keamanan pada website dengan metode pengujian penetrasi OWASP ZAP. *Jurnal RESISTOR (Rekayasa Sistem Komputer), 7*(3), 153–161. https://doi.org/10.31598/jurnalresistor.v7i3.1459

Setiawan, E., & Fachri, F. (2025). Pengujian dan mitigasi kerentanan website sistem informasi akademik Universitas Ma'arif Nahdlatul Ulama Kebumen dengan OWASP ZAP. https://doi.org/10.14421/csecurity.2025.8.1.5190

Sitorus, M. G. B., Maria, N., & Safa, Y. N. (2024). Tinjauan literatur manajemen risiko cyber dalam proyek: Identifikasi, evaluasi, dan mitigasi ancaman. *Jurnal Manajemen Informatika (JAMIKA), 14*(2), 187–198. https://doi.org/10.34010/jamika.v14i2.12887

Utami, G. C., Supramaji, A. B., & Isnaini, K. N. (2023). Penilaian risiko keamanan informasi pada website dengan metode DREAD dan ISO 27005:2018. *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia), 8*(1), 47–56. https://doi.org/10.32528/justindo.v8i1.219

Winarto, A. J., & Budi, S. (2024). Analisis manajemen risiko UMKM Fashion Bonoer Store Jombang di era pandemi. *Journal of Sharia Economics, Banking and Accounting, 1*(1), 20–29. https://doi.org/10.52620/jseba.v1i1.12

ZAP, M. O. Z. A. P. (2023). Vulnerability and mitigation analysis of the ITERA e-learning website using OWASP Zed Attack Proxy (ZAP). http://dx.doi.org/10.20884/1.dr.2023.19.1.533

e-ISSN : 3031-9943; dan p-ISSN : 3031-9935; Hal. 136-154