Jurnal Informatika Vol. 15, No. 1, Juni 2026, Page. 73~86
E-ISSN: 2528-0090 https://ejournal.unidayan.ac.id/index.php/JIU
P-ISSN: 2252-9160 DOI: https://doi.org/10.55340/jiu.v15i1.2711

ANALISIS RISIKO KEAMANAN INFORMASI PADA *WEBSITE* PERUSAHAAN MENGGUNAKAN ISO/IEC 27001 DAN ISO/IEC 27005

INFORMATION SECURITY RISK ASSESSMENT ON CORPORATE WEBSITES USING ISO/IEC 27001 AND ISO/IEC 27005

Muhammad Goldvin Wijayakusuma[1*], Nurhadi Surojudin[2], Sanudin[3]
[1,2,3]Program Studi Teknik Informatika, Universitas Pelita Bangsa, Bekasi, Indonesia
Email korespondensi: [1*]goldvinwijaya@gmail.com

Article Info:	Received	Revised	Accepted	Published:
	31 Mei 2026	01 Juni 2026	06 Juni 2026	06 Juni 2026

Abstrak

Website Document Management System (DMS) yang menyimpan dokumen sensitif seperti rekaman ISMS dan risk register kini menjadi infrastruktur inti operasional di banyak organisasi, namun eksposur risikonya terhadap aspek kerahasiaan, integritas, dan ketersediaan belum banyak diteliti secara teknis. Penelitian ini bertujuan untuk menganalisis risiko keamanan informasi pada Website DMS perusahaan menggunakan ISO/IEC 27005:2022 sebagai kerangka penilaian risiko dan ISO/IEC 27001:2022 Annex A sebagai acuan pemetaan kontrol. Penelitian berbasis standar sebelumnya umumnya mengandalkan wawancara atau kuesioner, tidak menyasar DMS dengan sensitivitas aset tinggi, dan menggunakan versi ISO pra-2022, sehingga temuan teknisnya sulit diverifikasi. Data dikumpulkan melalui wawancara terstruktur 18 pertanyaan kepada tiga peran pengelola sistem, observasi antarmuka aplikasi, dan validasi teknis non-invasif menggunakan SecurityHeaders.com serta inspeksi Response Header. Dari enam kategori aset dan sepuluh risiko berbasis CIA, lima dikategorikan tinggi (skor 12–15), empat sedang (skor 6–10), dan satu rendah. Validasi teknis mengungkap tiga temuan: inkonsistensi RBAC antara lapisan frontend dan backend sesuai OWASP A01:2021, kegagalan implementasi Security Header dengan grade F sesuai OWASP A05:2021, serta eksposur versi server nginx/1.18.0 pada Response Header. Pemetaan ke Annex A menghasilkan lima rekomendasi pengendalian mencakup kontrol 5.15, 8.5, 8.9, 8.13, serta 5.30 dan 8.14. Penelitian ini menunjukkan bahwa validasi teknis dapat diintegrasikan ke dalam alur ISO/IEC 27005:2022 untuk menghasilkan temuan yang lebih dapat diverifikasi dibandingkan pendekatan berbasis survei pada konteks DMS. Implikasi metodologisnya adalah potensi adopsi validasi teknis non-invasif sebagai bagian standar penilaian risiko pada sistem informasi sensitif serupa.

Kata Kunci: *Analisis Risiko; Corporate Website; DMS; ISO/IEC 27001; ISO/IEC 27005; Keamanan Informasi.*

Jurnal Informatika Vol. 15, No. 1, Juni 2026, Page. 73~86
E-ISSN: 2528-0090 https://ejournal.unidayan.ac.id/index.php/JIU
P-ISSN: 2252-9160 DOI: https://doi.org/10.55340/jiu.v15i1.2711

Abstract

Corporate Document Management Systems (DMS) storing sensitive assets such as ISMS records and risk registers occupy a central role in organizational operations, yet their exposure to confidentiality, integrity, and availability risks remains undercharacterized in technical empirical research. This study aimed to assess information security risks on a corporate DMS website using ISO/IEC 27005:2022 as the risk assessment framework and ISO/IEC 27001:2022 Annex A as the control mapping reference. Standard-based risk assessments in this domain have typically relied on interviews or questionnaires, have not targeted DMS environments with high asset sensitivity, and were conducted under pre-2022 ISO versions, limiting verifiability and technical depth. Data were collected through structured interviews of 18 standard-based questions to three system management roles, direct observation of the application interface, and non-invasive technical validation using SecurityHeaders.com with HTTP Response Header inspection. From six asset categories and ten CIA-mapped risks, five were high-risk (scores 12–15), four medium-risk (scores 6–10), and one low-risk. Technical validation identified three findings: RBAC inconsistency between frontend and backend layers per OWASP A01:2021, absent security headers producing Grade F per OWASP A05:2021, and server version nginx/1.18.0 exposed through the Response Header. Control mapping produced five recommendations covering controls 5.15, 8.5, 8.9, 8.13, and 5.30 together with 8.14. The study demonstrates that technical validation can be embedded within an ISO/IEC 27005:2022 workflow to produce more directly verifiable findings than survey-based approaches in DMS contexts. The methodological implication is that non-invasive technical validation holds potential as a standard component of risk assessments for similarly sensitive systems.

Keywords: *Risk Assessment; Corporate Website; DMS; ISO/IEC 27001; ISO/IEC 27005; Information Security.*

1. PENDAHULUAN

Ketergantungan organisasi terhadap sistem berbasis web terus tumbuh seiring percepatan transformasi digital. *Document Management System* (DMS) menjadi salah satu sistem yang banyak digunakan untuk menyimpan, mengelola, dan mendistribusikan dokumen dalam lingkup organisasi secara terpusat [1], [2], [3]. Ketergantungan yang tinggi terhadap sistem ini membuka celah risiko keamanan informasi yang perlu ditangani secara terstruktur, bukan sekadar dengan pendekatan teknis *ad hoc*.

Laporan Keamanan Siber Indonesia yang diterbitkan oleh Badan Siber dan Sandi Negara pada tahun 2023 mencatat peningkatan insiden siber di berbagai sektor organisasi [4], [5] menegaskan bahwa biaya rata-rata kebocoran data global telah mencapai USD 4,35 juta pada tahun 2022 dan *cybercrime* diprediksi terus meningkat secara signifikan [21]. Sistem DMS yang menyimpan dokumen sensitif seperti laporan keuangan, data pelanggan, dan informasi operasional menjadi sasaran serangan seperti *unauthorized access*, *SQL Injection*, *Cross-Site Scripting* (XSS), dan *malware injection* [1], [6], [20]. Data OWASP Top 10:2021 menunjukkan bahwa *Broken Access Control* (A01) ditemukan pada 94 persen aplikasi web yang diuji, sementara *Security Misconfiguration* (A05) terdeteksi pada 90 persen aplikasi [7]. Kedua jenis kerentanan ini kembali menjadi perhatian dalam OWASP Top 10:2025 yang mengonfirmasi bahwa tantangan keamanan web tetap konsisten selama beberapa siklus berturut-turut [8], [19].

Vol. 15, No. 1, Juni 2026, Page. 73~86
https://ejournal.unidayan.ac.id/index.php/JIU
DOI: https://doi.org/10.55340/jiu.v15i1.2711

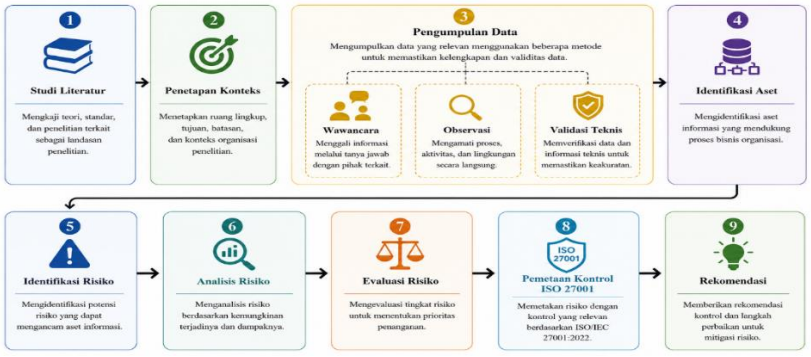
Berbagai penelitian telah menerapkan standar ISO/IEC 27001 dan ISO/IEC 27005 dalam analisis risiko keamanan informasi di berbagai konteks. Chandra et al. (2022) menunjukkan bahwa pendekatan berbasis *framework* standar internasional menghasilkan analisis yang lebih terstruktur dan dapat direplikasi [9], [22]. Hidayatullah, Kunthi and Harwahyu (2024) menerapkan ISO/IEC 27005:2022 pada *Audit Management System* dan menghasilkan pemetaan risiko yang komprehensif terhadap aset serta proses internal audit [10]. Irfan et al. (2025) mengaplikasikan ISO/IEC 27005 pada sistem *e-learning* dengan dukungan arsitektur *blockchain* [11], sedangkan Hikam, Dewi and Praditya (2024) menggunakan ISO/IEC 27005:2018 untuk mengidentifikasi ancaman utama dan menyusun *action plan* pengendalian risiko pada PT XYZ [12]. Chandra and Yusuf (2025) secara khusus mengaplikasikan ISO/IEC 27005:2022 pada penilaian risiko aplikasi web layanan organisasi, yang relevansinya paling dekat dengan konteks penelitian ini [13].

Meskipun penelitian-penelitian tersebut memberikan kontribusi penting, terdapat tiga kesenjangan yang belum terjawab. Pertama, sebagian besar penelitian mengandalkan wawancara atau kuesioner tanpa pemeriksaan teknis aktual, sehingga kerentanan nyata pada lapisan aplikasi belum terungkap. Kedua, penelitian yang khusus menyasar DMS dengan dokumen sensitif (ISMS, *risk register*) masih sangat jarang, padahal sensitivitas asetnya jauh lebih tinggi dibanding aplikasi web umum [2], [3]. Ketiga, kajian yang menerapkan ISO/IEC 27005:2022 bersama ISO/IEC 27001:2022 secara konsisten masih terbatas. Ketiga celah ini menjadi justifikasi penelitian ini. Kombinasi kedua standar dipilih karena ISO/IEC 27005:2022 dirancang sebagai panduan manajemen risiko untuk mendukung implementasi ISO/IEC 27001 [14], [15], sehingga penggunaannya bersama menjamin konsistensi penilaian risiko dan pengendalian. Putra and Soewito (2023) [17] memperkuat pilihan kombinasi standar tersebut dengan menunjukkan bahwa penggunaan dua framework secara terpadu menghasilkan cakupan analisis risiko yang lebih lengkap dan komprehensif dibandingkan penggunaan satu framework secara tunggal.

Penelitian ini bertujuan untuk menganalisis risiko keamanan informasi pada *Website* DMS perusahaan menggunakan ISO/IEC 27005:2022, kemudian memetakan setiap risiko terhadap kontrol Annex A ISO/IEC 27001:2022 sebagai dasar rekomendasi pengendalian. Kontribusi utama penelitian ini adalah kerangka analisis berbasis bukti teknis langsung pada sistem DMS, yang mengisi kesenjangan metodo*log*is dibanding penelitian berbasis survei semata.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode analisis risiko keamanan informasi berbasis ISO/IEC 27005:2022. Objek penelitian adalah *Website Document Management System* (DMS) milik sebuah perusahaan yang mengelola dokumen ISMS, *risk register*, dan aset informasi organisasi. Identitas perusahaan dianonimkan sesuai kesepakatan kerahasiaan yang telah ditetapkan bersama. Penelitian dilakukan melalui beberapa tahapan yang saling berkaitan sebagaimana digambarkan pada Gambar 1.



Gambar 1. Diagram Alur Metodologi Penelitian

2.1 Metode Pengumpulan Data

Pengumpulan data menggunakan empat pendekatan: (1) studi literatur terhadap ISO/IEC 27001:2022 dan ISO/IEC 27005:2022 [14], [15], implementasi ISO/IEC 27001 pada sektor TI [16], serta berbagai penelitian terkait manajemen risiko keamanan informasi, aplikasi web, dan DMS [9], [10], [11], [12], [13]. (2) wawancara terstruktur 18 pertanyaan berbasis klausul ISO/IEC 27001:2022 dan ISO/IEC 27005:2022 Annex B kepada tiga peran pengelola sistem; (3) observasi langsung antarmuka aplikasi, autentikasi, hak akses, dan kontrol keamanan tanpa eksploitasi aktif; (4) validasi teknis *non-invasif* menggunakan SecurityHeaders.com, inspeksi *Response Header*, pengujian *session management* pasif, dan verifikasi HTTPS/SSL.

2.2 Batasan Penelitian

Penelitian ini memiliki empat batasan: (1) cakupan terbatas pada lapisan aplikasi web DMS; (2) validasi teknis *non-invasif* tanpa *VAPT* formal; (3) penilaian risiko *semi-kuantitatif* tanpa data historis insiden; dan (4) identitas organisasi dianonimkan. Batasan-batasan ini mencerminkan ruang lingkup penelitian yang ditetapkan dan diakui sebagai keterbatasan yang perlu diperhatikan dalam interpretasi temuan.

2.3 Tahapan Analisis Risiko ISO/IEC 27005

Analisis risiko mengikuti alur ISO/IEC 27005:2022 yang terdiri dari lima tahap. Tahap pertama adalah penetapan konteks risiko, yang mendefinisikan ruang lingkup, aset yang perlu dilindungi, kriteria evaluasi, dan batasan penelitian. Tahap kedua adalah identifikasi risiko, yaitu mengidentifikasi aset, ancaman, kerentanan, dan konsekuensi berdasarkan hasil pengumpulan data. Identifikasi ancaman mengacu pada katalog *ISO/IEC 27005:2022 Annex C dan OWASP Top 10:2021 [7], [14], [15]*. Tahap ketiga adalah analisis risiko, di mana nilai Likelihood (L) dan Impact (I) ditentukan secara *semi-kuantitatif* menggunakan skala 1 sampai 5 dengan rubrik terstandar. Nilai risiko dihitung menggunakan rumus berikut.

$$Risk\ Score = Likelihood\ (L) \times Impact\ (I) \quad (1)$$

Penentuan nilai Likelihood mempertimbangkan kondisi aktual keamanan sistem dari hasil validasi teknis, frekuensi historis ancaman sejenis berdasarkan laporan BSSN dan perkembangan ancaman siber dalam literatur terbaru [4], [5], serta kondisi kerentanan yang ditemukan. Penentuan nilai Impact mempertimbangkan dampak terhadap tiga dimensi CIA (*Confidentiality, Integrity, Availability*), ketergantungan operasional terhadap aset terdampak, dan nilai bisnis aset bagi organisasi. Tahap keempat adalah evaluasi risiko, yaitu mengelompokkan nilai risiko ke dalam tiga kategori untuk menentukan prioritas penanganan. Tahap kelima adalah pemetaan kontrol, yaitu menghubungkan setiap risiko dengan kontrol *Annex A ISO/IEC 27001:2022* yang relevan sebagai dasar rekomendasi.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Wawancara dan Observasi

Wawancara terstruktur dilaksanakan kepada tiga peran pengelola sistem sebagai narasumber dalam pengelolaan sistem DMS. Hasilnya menunjukkan bahwa sistem telah menerapkan kontrol keamanan dasar yang cukup memadai. Autentikasi pengguna berbasis *username-password*, pembatasan hak akses berbasis *role* (*RBAC*), pencatatan aktivitas, *backup* data, dan penggunaan *HTTPS* semuanya telah berjalan. Namun, beberapa kontrol masih berada pada tahap perencanaan, di antaranya kebijakan keamanan informasi secara formal dan pelaksanaan *vulnerability assessment* berkala.

Observasi langsung mengonfirmasi implementasi mekanisme keamanan dasar tersebut. Temuan penting dari observasi adalah ketidakkonsistenan antara pembatasan akses di sisi *frontend* dan *backend*. *Role Asset Owner* masih dapat membuka halaman *Settings* dan mengakses form konfigurasi meskipun proses penyimpanan akhirnya ditolak oleh *backend*. Kondisi ini menciptakan potensi kebocoran informasi mengenai struktur sistem yang seharusnya tidak terekspos kepada pengguna

dengan peran tersebut, dan temuan ini konsisten dengan yang dilaporkan [18],[7],[9] terkait pentingnya konsistensi kontrol antara lapisan *frontend* dan *backend*.

3.2 Hasil Validasi Keamanan

Validasi keamanan secara teknis dilakukan terhadap 19 aspek pemeriksaan yang dikelompokkan ke dalam delapan kategori menggunakan pendekatan *non-invasif*, yaitu *HTTPS* dan Komunikasi Data, Autentikasi, Hak Akses, *Input Validation*, *Error Handling*, *Security Header*, *Logging* dan *Monitoring*, *Backup* dan *Recovery*, serta Konfigurasi Sistem [14], [15]. Hasil pemeriksaan lengkap disajikan pada Tabel 1 di bawah ini.

Tabel 1. Hasil Validasi Keamanan

No	Kategori Pemeriksaan	Pemeriksaan	Tujuan Validasi	Hasil Observasi	Status
1	HTTPS & Komunikasi Data	*Website* menggunakan HTTPS	Enkripsi komunikasi data	HTTPS aktif dengan sertifikat SSL valid	Sesuai
2	HTTPS & Komunikasi Data	Sertifikat SSL/TLS aktif dan valid	Cegah warning browser	Sertifikat valid, tanpa warning browser	Sesuai
3	Autentikasi	Terdapat halaman *login*	Verifikasi autentikasi pengguna	*Login* berbasis *username* dan *password* tersedia	Sesuai
4	Autentikasi	*Password* tidak tampil secara *plaintext*	Lindungi kerahasiaan *password*	*Password* ditampilkan sebagai karakter tersembunyi	Sesuai
5	Autentikasi	*Session logout* berjalan dengan baik	Cegah *session hijacking*	*Session* berakhir setelah *logout*, akses memerlukan *login* ulang	Sesuai
6	Hak Akses	*Role* user berjalan sesuai hak akses	Verifikasi implementasi *access control*	Tombol aksi modul lain masih tampil untuk *role* Asset Owner meski penyimpanan ditolak *backend*	Perlu Perbaikan
7	Hak Akses	User tidak dapat mengakses halaman admin	Cegah *privilege escalation*	*Role Asset* Owner dapat membuka halaman Settings dan form konfigurasi; penyimpanan ditolak *backend*	Perlu Perbaikan
8	*Input Validation*	Form input memiliki validasi dasar	Kurangi risiko input tidak valid	Validasi field wajib dan format input berjalan sebelum data disimpan	Sesuai
9	*Input Validation*	Input karakter khusus ditangani sistem	Kurangi potensi XSS/Injection	Script pada form input tidak dieksekusi dan tidak memicu error aplikasi	Sesuai
10	*Error Handling*	Error system tidak menampilkan informasi sensitif	Cegah *information disclosure*	Hanya pesan error umum ditampilkan, tanpa detail teknis	Sesuai
11	*Security Header*	Terdapat *Security Header* dasar	Tingkatkan keamanan aplikasi web	*Security Header* dasar tidak diterapkan, *grade F* pada SecurityHeaders.com	Perlu Perbaikan
12	*Security Header*	Header *server* tidak menampilkan informasi berlebihan	Kurangi *fingerprinting* server	*Response Header* mengekspos versi server: nginx/1.18.0 (Ubuntu)	Perlu Perbaikan
13	*Logging & Monitoring*	Aktivitas *login* tercatat	Dukung *monitoring*	*Login* pengguna tercatat pada menu *log* aktivitas	Sesuai

			aktivitas pengguna		
14	*Logging & Monitoring*	Aktivitas penting dapat dipantau	Dukung *audit trail*	Aktivitas *login* dan perubahan data tercatat dan dapat ditelusuri	Sesuai
15	*Backup & Recovery*	Terdapat mekanisme *Backup*	Kurangi risiko kehilangan data	Fitur ekspor data ISMS tersedia sebagai *backup* manual melalui menu Data & *Backup*	Sesuai
16	*Backup & Recovery*	Terdapat mekanisme *recovery*	Pastikan data dapat dipulihkan	*Recovery* tersedia melalui file *backup* ekspor data saat terjadi gangguan	Sesuai
17	Konfigurasi Sistem	*Website* tidak menampilkan *directory listing*	Cegah akses file sensitif	*Directory listing* tidak ditampilkan pada path direktori umum	Sesuai
18	Konfigurasi Sistem	Tidak ditemukan *debug mode* pada *production*	Kurangi risiko disclosure informasi	*Debug mode* dan detail teknis tidak tampil di lingkungan *production*	Sesuai
19	*Session Management*	*Session* tidak dapat digunakan ulang setelah *logout*	Cegah *session* abuse	*Session* tidak dapat digunakan ulang setelah *logout*, diarahkan ke halaman *login*	Sesuai

Dari 19 aspek yang diperiksa, 15 berstatus Sesuai dan 4 Perlu Perbaikan, seluruhnya pada kategori Hak Akses (aspek 6-7) dan *Security Header* (aspek 11-12). Temuan ini menjadi dasar penetapan risiko: *Grade F Security Header* (Risiko 5), eksposur versi *server* (Risiko 4), dan inkonsistensi *access control* (Risiko 1, 2, dan 3).

3.3 Identifikasi Aset

Berdasarkan hasil pengumpulan data, aset pada sistem DMS dikelompokkan ke dalam enam kategori sebagaimana ditunjukkan pada Tabel 2. Keenam aset ini dipilih karena secara langsung berpengaruh terhadap kerahasiaan, integritas, dan ketersediaan informasi pada sistem [3], [14].

Tabel 2. Identifikasi Aset DMS

No	Kategori Aset	Nama Aset	Deskripsi
1	Aplikasi	Aplikasi DMS	Aplikasi web utama pengelolaan dokumen dan informasi keamanan organisasi
2	Informasi	Data dan Informasi DMS	Dokumen ISMS, *risk register*, data aset, dan informasi operasional
3	Pengguna	Akun Pengguna dan Hak Akses	Akun pengguna dengan *role RBAC* dari sekitar 50 pengguna aktif
4	Database	Database PostgreSQL	Penyimpanan data utama: dokumen, pengguna, dan *log* aktivitas
5	*Backup*	*Backup* Data	Salinan data untuk pemulihan saat terjadi kegagalan sistem
6	Infrastruktur	Web Server dan Infrastruktur	Server nginx/1.18.0 dan komponen jaringan pendukung aplikasi DMS berbasis *cloud*

3.4 Identifikasi Risiko

Identifikasi risiko dilakukan dengan menghubungkan aset, ancaman, dan kerentanan berdasarkan hasil pengumpulan data dan validasi teknis. Ancaman pada Risiko nomor 10 diidentifikasi sebagai penyalahgunaan data *log* oleh pihak yang tidak berwenang, karena *log* aktivitas berisi informasi sensitif yang berpotensi dieksploitasi untuk serangan lanjutan apabila akses terhadapnya tidak dibatasi secara granular. Hasil identifikasi disajikan pada Tabel 3.

Tabel 3. Identifikasi Risiko

No	CIA	Aset	Ancaman	Kerentanan	Risiko
1	C	Data dan Info DMS	Akses tidak sah (OWASP A01)	*RBAC frontend* tidak konsisten dengan *backend*	Kebocoran dokumen penting

2	I	Data dan Info DMS	Manipulasi data	Fitur aksi tampil pada *role* tidak terotorisasi	Perubahan data tanpa otorisasi
3	C	Akun Pengguna	*Credential compromise*	Autentikasi hanya *username-password* tanpa MFA	Akses tidak sah ke sistem
4	C	Web Server	*Information disclosure* via *fingerprinting*	nginx/1.18.0 terekspos di *Response Header*	*Fingerprinting* server
5	I	Aplikasi DMS	Serangan web (OWASP A05)	*Security Header* belum diterapkan (*Grade F*, SecurityHeaders.com)	Peningkatan risiko serangan web
6	A	Database PostgreSQL	Kegagalan atau serangan database	Satu instance database tanpa *failover*	Gangguan layanan sistem
7	A	*Backup* Data	Kegagalan *recovery* data	*Backup* manual via ekspor data; tidak ada pengujian *restore* berkala	Kehilangan atau kerusakan data
8	I	Data dan Info DMS	*Human error*	Tidak ada *versioning* dokumen dan konfirmasi penghapusan berlapis	Perubahan atau penghapusan dokumen tidak disengaja
9	A	*Web Server*	*Downtime* server atau serangan *DDoS*	Infrastruktur *cloud* tanpa redundansi eksplisit	Layanan sistem tidak tersedia
10	C	Data dan Info DMS	Penyalahgunaan *log* oleh pihak tidak berwenang	Akses *log* aktivitas tidak dibatasi granular per peran pengguna	Kebocoran informasi aktivitas pengguna

Keterangan: C = *Confidentiality*; I = *Integrity*; A = *Availability*

3.5 Analisis Risiko

Penilaian risiko dilakukan menggunakan rubrik *Likelihood* dan Impact masing-masing berskala 1 sampai 5 sebagaimana ditunjukkan pada Tabel 4 dan Tabel 5. Nilai *Likelihood* ditentukan berdasarkan kondisi aktual dari hasil validasi teknis, data referensi ancaman dari BSSN dan perkembangan ancaman siber dalam literatur terbaru [4], [5], serta kondisi kerentanan aktual yang ditemukan. Nilai *Impact* ditentukan berdasarkan dampak terhadap ketiga dimensi CIA, ketergantungan operasional terhadap aset terdampak, dan nilai bisnis aset bagi organisasi.

Tabel 4. Skala Likelihood dan Kriteria Penetapan Nilai

Nilai	Keterangan	Kriteria Justifikasi
1	Sangat Tidak Mungkin	Tidak ada bukti ancaman dan kontrol pencegahan sangat kuat serta sudah diuji secara berkala
2	Tidak Mungkin	Ancaman diketahui namun kontrol yang ada cukup efektif membatasinya dan tidak ada indikasi eksploitasi aktif
3	Mungkin	Kerentanan teridentifikasi dari validasi teknis, ancaman diketahui aktif secara umum berdasarkan BSSN dan OWASP, serta kontrol yang ada tidak konsisten
4	Kemungkinan Besar	Kerentanan terkonfirmasi dengan bukti teknis, ancaman sangat umum, dan kontrol yang tersedia lemah atau tidak ada
5	Sangat Mungkin	Eksploitasi aktif sudah terdokumentasi, tidak ada kontrol pencegahan, dan kerentanan kritis sudah terkonfirmasi

Tabel 5. Skala Impact dan Kriteria Penetapan Nilai

Nilai	Keterangan	Kriteria Dampak terhadap CIA dan Operasional
1	Sangat Kecil	Dampak minimal terhadap CIA dan tidak mengganggu operasional, pemulihan bisa dilakukan secara instan
2	Kecil	Gangguan minor pada salah satu aspek CIA, operasional sedikit terganggu, dan pemulihan mudah dilakukan

3	Sedang	Gangguan nyata pada salah satu aspek CIA, operasional terganggu secara parsial, dan diperlukan tindakan korektif
4	Besar	Gangguan pada dua aspek CIA, operasional terganggu secara substansial, dan pemulihan memerlukan waktu serta sumber daya
5	Sangat Besar	Kompromi pada seluruh aspek CIA, operasional terhenti, dan berpotensi menimbulkan kerugian finansial, reputasi, serta kepatuhan hukum yang signifikan

Kategorisasi risiko menggunakan $Risk\ Score = L \times I$ dengan tiga kategori: Rendah (1-5, *monitoring* berkala), Sedang (6-10, pengendalian dan *monitoring*), dan Tinggi (11-25, tindakan segera). Hasil evaluasi seluruh risiko disajikan pada Tabel 6.

Tabel 6. Hasil Analisis Risiko dengan Justifikasi Penetapan Nilai

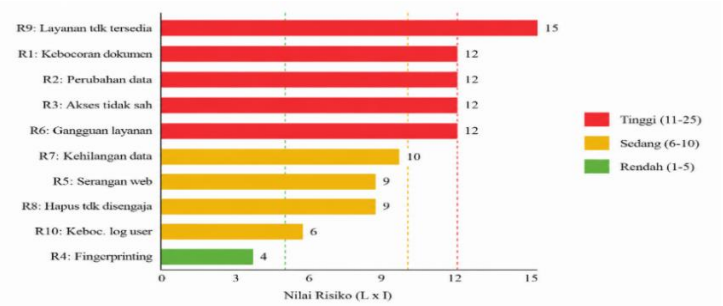
No	Risiko	L	I	L×I	Kategori	Justifikasi Penetapan Nilai L dan I
1	Kebocoran dokumen penting	3	4	**12**	Tinggi	L=3: *RBAC frontend* rentan (terkonfirmasi validasi); *Broken Access Control* ada di 94% aplikasi web [8]. I=4: dokumen ISMS dan *risk register* sangat sensitif; kebocoran berdampak langsung pada Confidentiality dan reputasi.
2	Perubahan data tanpa otorisasi	3	4	**12**	Tinggi	L=3: validasi mengonfirmasi *role* Asset Owner dapat mengakses form Settings tanpa otorisasi yang sesuai. I=4: perubahan data ISMS melanggar Integrity dokumen audit dan mengganggu kepatuhan organisasi [14].
3	Akses tidak sah ke sistem	3	4	**12**	Tinggi	L=3: autentikasi *single-factor* tanpa MFA rentan terhadap *credential compromise*. I=4: akses tidak sah memungkinkan eksfiltrasi seluruh dokumen organisasi [15].
4	*Fingerprinting* server	2	2	**4**	Rendah	L=2: versi server terekspos di header (terkonfirmasi); *fingerprinting* tidak langsung menyebabkan kompromi. I=2: dampak langsung kecil; berfungsi sebagai *enabler* risiko lanjutan.
5	Peningkatan risiko serangan web	3	3	**9**	Sedang	L=3: SecurityHeaders.com menghasilkan *Grade F*; CSP, X-Frame-Options, dan header lain tidak tersedia (terkonfirmasi). I=3: eksploitasi memerlukan langkah tambahan; dampak bergantung pada jenis serangan yang berhasil dijalankan.
6	Gangguan layanan sistem	3	4	**12**	Tinggi	L=3: sistem bergantung pada layanan *cloud* tunggal; ancaman *downtime* dan *DDoS* umum terjadi. I=4: gangguan menghentikan akses semua pengguna ke dokumen operasional.
7	Kehilangan atau kerusakan data	2	5	**10**	Sedang	L=2: *backup* tersedia namun manual; belum ada pengujian *restore* terdokumentasi. I=5: kehilangan data ISMS berdampak besar pada kepatuhan dan keberlangsungan operasional.
8	Perubahan/penghapusan dokumen tidak disengaja	3	3	**9**	Sedang	L=3: *human error* umum terjadi; belum ada kontrol versi dokumen. I=3: hilangnya dokumen individual berdampak sedang; dokumen lain masih dapat diakses.
9	Layanan sistem tidak tersedia	3	5	**15**	Tinggi	L=3: infrastruktur *cloud* tanpa redundansi eksplisit; serangan *DDoS* meningkat [4]. I=5: ketidaktersediaan

Vol. 15, No. 1, Juni 2026, Page. 73~86
https://ejournal.unidayan.ac.id/index.php/JIU
DOI: https://doi.org/10.55340/jiu.v15i1.2711

						sistem menghentikan seluruh operasional pengelolaan dokumen.
10	Kebocoran informasi aktivitas pengguna	2	3	**6**	Sedang	L=2: data *log* tersedia namun belum dibatasi aksesnya secara granular. I=3: eksposur *log* mengungkap pola aktivitas sensitif tanpa mengekspos isi dokumen secara langsung.

Tabel 6 menyajikan penilaian sepuluh risiko pada *Website* DMS menggunakan formulasi *Risk Score* = L × I, dengan L (*Likelihood*) dan I (Impact) berskala 1-5 berdasarkan kondisi teknis aktual dan potensi dampak terhadap aspek CIA [3], [15].

Tiga contoh representatif: (1) Tinggi: Risiko 1 (Kebocoran Dokumen) skor 12 (L=3 kerentanan *RBAC* terkonfirmasi; I=4 dokumen ISMS/*risk register* sangat sensitif); (2) Sedang: Risiko 5 (Serangan Web) skor 9 (L=3 *Grade F Security Header*; I=3 dampak bergantung jenis serangan); (3) Rendah: Risiko 4 (*Fingerprinting Server*) skor 4 (L=2 *nginx/1.18.0* terekspos; I=2 hanya *enabler* risiko lanjutan).



Gambar 2. Diagram Batang Nilai Risiko Berdasarkan Likelihood × Impact

Gambar 2 menunjukkan distribusi nilai risiko dari seluruh risiko yang teridentifikasi, diurutkan dari nilai tertinggi ke terendah. Lima risiko dengan nilai di atas 11 masuk kategori tinggi, empat risiko dengan nilai 6 sampai 10 masuk kategori sedang, dan satu risiko dengan nilai di bawah 6 masuk kategori rendah. Risiko nomor 9 tentang layanan sistem tidak tersedia memper*oleh* nilai tertinggi sebesar 15 karena kombinasi antara dampak yang sangat besar (I=5) akibat ketergantungan penuh pada satu infrastruktur *cloud* dengan probabilitas yang cukup tinggi (L=3) mengingat tidak adanya redundansi yang dikonfigurasi secara eksplisit.

3.6 Evaluasi Risiko

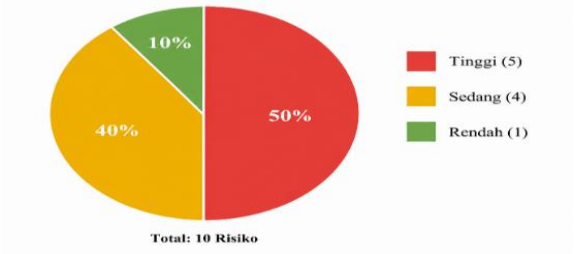
Evaluasi risiko dilakukan untuk menentukan prioritas penanganan berdasarkan hasil analisis pada Tabel 6. Hasilnya disajikan pada Tabel 7, dilengkapi dengan visualisasi distribusi kategori risiko pada Gambar 3 dan peta matriks risiko pada Gambar 4.

Tabel 7. Evaluasi Risiko dan Prioritas Penanganan

No	Risiko	Skor	Kategori	Prioritas Penanganan
1	Kebocoran dokumen penting	12	Tinggi	Prioritas Utama: konsistensi *RBAC* antara *frontend* dan *backend*
2	Perubahan data tanpa otorisasi	12	Tinggi	Prioritas Utama: validasi hak akses ketat pada setiap proses perubahan data
3	Akses tidak sah ke sistem	12	Tinggi	Prioritas Utama: implementasi *Multi-Factor Authentication* dan kebijakan *password* yang kuat
4	*Fingerprinting* server	4	Rendah	*Monitoring*: sembunyikan versi nginx di *Response Header* menggunakan konfigurasi *server_tokens off*
5	Peningkatan risiko serangan web	9	Sedang	Pengendalian dan *Monitoring*: terapkan *Security Header* dasar meliputi CSP, X-Frame-Options, dan HSTS

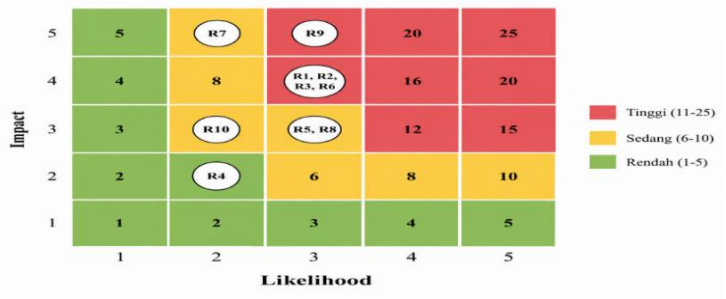
6	Gangguan layanan sistem	12	Tinggi	Prioritas Utama: *monitoring* infrastruktur, *rate limiting*, dan *auto-restart* layanan
7	Kehilangan atau kerusakan data	10	Sedang	Pengendalian dan *Monitoring*: otomatisasi *backup* harian dan pengujian *restore* secara triwulanan
8	Perubahan/penghapusan dokumen tidak disengaja	9	Sedang	Pengendalian dan *Monitoring*: implementasikan kontrol versi dokumen dan konfirmasi ganda sebelum penghapusan
9	Layanan sistem tidak tersedia	15	Tinggi	Prioritas Tertinggi: susun *Business Continuity Plan* dengan RTO dan RPO terdefinisi serta implementasikan redundansi infrastruktur
10	Kebocoran informasi aktivitas pengguna	6	Sedang	Pengendalian dan *Monitoring*: batasi akses *log* hanya kepada administrator keamanan dan terapkan enkripsi *log*

Tabel 7 mengelompokkan sepuluh risiko ke dalam tiga kategori: 5 risiko Tinggi (skor 12-15), 4 risiko Sedang (skor 6-10), dan 1 risiko Rendah (skor di bawah 6). Risiko nomor 9 (Layanan Tidak Tersedia) memperoleh skor tertinggi 15 (L=3, I=5), memerlukan *Business Continuity Plan* dengan RTO/RPO terdefinisi dan redundansi infrastruktur [15], [14]. Risiko nomor 7 (Kehilangan Data) menjadi prioritas Sedang dengan skor 10 (L=2, I=5), direkomendasi otomatisasi *backup* dan pengujian *restore* triwulanan. Risiko nomor 4 (*Fingerprinting* Server) memperoleh skor terendah 4 (L=2, I=2), cukup ditangani dengan konfigurasi *server_tokens off*. Hasil evaluasi ini menjadi dasar pemetaan kontrol ISO/IEC 27001:2022 pada bagian berikutnya.



Gambar 3. Distribusi Proporsi Kategori Risiko

Gambar 3 menunjukkan distribusi kategori risiko: 50% (5 risiko) berkategori Tinggi, meliputi kebocoran dokumen, perubahan data tanpa otorisasi, akses tidak sah, gangguan layanan, dan layanan tidak tersedia; 40% (4 risiko) berkategori Sedang; dan 10% (1 risiko) berkategori Rendah. Dominasi risiko Tinggi mengindikasikan perlunya prioritisasi pengendalian pada aspek *access control* dan ketersediaan layanan.



Gambar 4. Matriks Risiko 5×5 (Likelihood × Impact)

Gambar 4 memperlihatkan sebaran risiko pada matriks 5×5 berdasarkan nilai *Likelihood* dan Impact. Empat risiko (R1, R2, R3, R6) mengelompok pada koordinat Likelihood=3 dan Impact=4, yang mencerminkan risiko-risiko yang bersumber dari kelemahan *access control*. Risiko R9 menempati koordinat tertinggi pada *Likelihood*=3 dan *Impact*=5, sementara R7 berada di koordinat *Likelihood*=2 dan *Impact*=5, mencerminkan skenario di mana kemungkinan terjadi relatif rendah namun dampaknya sangat besar apabila benar-benar terjadi.

3.7 Pemetaan Risiko terhadap Kontrol ISO/IEC 27001:2022

Pemetaan risiko terhadap kontrol Annex A ISO/IEC 27001:2022 menghasilkan rekomendasi tindakan yang spesifik sebagaimana ditunjukkan pada Tabel 8.

Tabel 8. Pemetaan Risiko, Kontrol ISO/IEC 27001:2022, dan Rekomendasi Tindakan Spesifik

No	Risiko	Kontrol ISO 27001	Prioritas	Rekomendasi Tindakan Spesifik
1	Kebocoran dokumen penting	5.15, 5.18	Tinggi	Terapkan *deny by default* di *frontend* per *role*; sembunyikan fitur tidak terotorisasi, bukan hanya blokir di *backend*
2	Perubahan data tanpa otorisasi	5.15, 8.5	Tinggi	Tambahkan validasi otorisasi *server-side* di setiap *endpoint* modifikasi; implementasikan *audit trail* dengan identitas pengguna dan *timestamp*
3	Akses tidak sah ke sistem	8.5, 8.15	Tinggi	Implementasikan MFA untuk semua akun; terapkan *account lockout* setelah 5 *login* gagal; aktifkan *monitoring* anomali autentikasi
4	*Fingerprinting* server	8.9	Rendah	Tambahkan *server_tokens off* pada konfigurasi nginx; upgrade ke versi *nginx* LTS terbaru untuk menutup *CVE* pada *nginx* 1.18.0
5	Peningkatan risiko serangan web	8.9	Sedang	Tambahkan CSP, *X-Frame-Options* (DENY), X-*Content-Type-Options* (*nosniff*), HSTS, dan Permissions-Policy pada konfigurasi *nginx*
6	Gangguan layanan sistem	5.30, 8.14	Tinggi	Implementasikan *monitoring uptime* otomatis, *auto-restart* layanan, dan *rate limiting* untuk mitigasi *DDoS*
7	Kehilangan atau kerusakan data	8.13	Sedang	Otomatisasi *backup* harian; uji prosedur *restore* triwulanan; simpan salinan di lokasi terpisah
8	Perubahan/penghapusan dokumen tidak disengaja	5.15, 8.15	Sedang	Implementasikan *versioning* dokumen; tambahkan konfirmasi berlapis sebelum penghapusan; terapkan *soft-delete* dengan retensi minimal 30 hari
9	Layanan sistem tidak tersedia	5.30, 8.14	Tertinggi	Susun BCP dengan RTO/RPO terdefinisi; implementasikan redundansi infrastruktur aktif-pasif; lakukan simulasi pemulihan berkala
10	Kebocoran informasi aktivitas pengguna	8.15, 5.34	Sedang	Batasi akses *log* hanya untuk administrator keamanan; implementasikan enkripsi *log*; terapkan kebijakan retensi *log* sesuai regulasi yang berlaku

3.8 Pembahasan

Sistem DMS memiliki fondasi kontrol keamanan dasar yang memadai, namun masih memerlukan penguatan pada area kritis. Temuan ini sejalan dengan [9], [10] yang menunjukkan bahwa sistem berbasis web umumnya rentan pada *access control* dan konfigurasi keamanan, dikonfirmasi OWASP yang menempatkan *Broken Access Control* sebagai risiko teratas pada siklus 2021 dan 2025 [7], [8]. Dari sisi Confidentiality, inkonsistensi akses antara *frontend* dan *backend* menciptakan kebocoran informasi struktur sistem meskipun *backend* menolak data tidak terotorisasi. Sahira et al. (2025) menegaskan bahwa konsistensi kontrol *frontend-backend* merupakan komponen kritis keamanan aplikasi web [18]. Hikam et al. (2024) menambahkan bahwa *logging* efektif dan *access control* terpadu merupakan landasan utama integritas data pada sistem informasi [12]. Dari sisi Integrity, risiko perubahan data tanpa otorisasi mengindikasikan perlunya *audit trail* yang komprehensif. Melaku (2023) dan Fahrurozi et al. (2020) menunjukkan bahwa *logging* adaptif merupakan kontrol efektif dalam kerangka ISO/IEC 27005 [25], [23]. Dari sisi Availability, Risiko nomor 9 memper*oleh* skor tertinggi (15) akibat ketergantungan penuh pada infrastruktur *cloud* tanpa *Business Continuity Plan* dan redundansi eksplisit. Melaku (2023) melaporkan bahwa BCP yang

memadai dapat mengurangi dampak gangguan layanan secara signifikan [25]. Kondisi ini memerlukan perhatian segera mengingat besarnya dampak operasional apabila layanan terhenti. Temuan teknis berupa *Grade F Security Header* dan eksposur *nginx/1.18.0* memetakan langsung ke A05:2021 *Security Misconfiguration* dan A01:2021 *Broken Access Control* pada OWASP Top 10:2021 [7], sehingga memperkuat nilai metodo*log*is penelitian ini dibanding pendekatan survei semata [24]. Adapun keterbatasan mencakup subjektivitas penilaian Likelihood dan Impact meskipun dipandu rubrik terstandar, serta cakupan validasi teknis yang *non-invasif* sehingga tidak mencakup seluruh permukaan serangan yang ada.

4. KESIMPULAN

Penelitian ini berhasil menganalisis risiko keamanan informasi pada Website DMS perusahaan menggunakan ISO/IEC 27005:2022 dan memetakannya ke kontrol Annex A ISO/IEC 27001:2022. Dari enam kategori aset dan sepuluh risiko berbasis CIA, ditemukan lima risiko kategori tinggi (skor 12–15), empat risiko kategori sedang (skor 6–10), dan satu risiko kategori rendah. Validasi teknis mengungkap tiga temuan utama: inkonsistensi RBAC antara lapisan frontend dan backend (OWASP A01:2021), kegagalan implementasi Security Header dengan grade F (OWASP A05:2021), serta eksposur versi server nginx/1.18.0 pada Response Header. Pemetaan ke Annex A ISO/IEC 27001:2022 menghasilkan lima rekomendasi pengendalian yang mencakup kontrol 5.15, 8.5, 8.9, 8.13, serta 5.30 dan 8.14.

Kontribusi metodologis utama penelitian ini adalah pembuktian bahwa integrasi validasi teknis non-invasif ke dalam alur ISO/IEC 27005:2022 menghasilkan temuan yang lebih dapat diverifikasi secara langsung dibandingkan pendekatan berbasis survei, sehingga memperkuat reliabilitas penilaian risiko pada konteks DMS dengan sensitivitas aset tinggi.

Penelitian ini memiliki keterbatasan berupa penilaian Likelihood dan Impact yang bersifat semi-kuantitatif serta cakupan validasi yang non-invasif tanpa pengujian penetrasi formal. Penelitian lanjutan disarankan mencakup Vulnerability Assessment and Penetration Testing (VAPT) formal, perluasan cakupan ke sistem informasi serupa lainnya, serta penggunaan data insiden historis untuk meningkatkan akurasi penilaian risiko.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Teknik Informatika Universitas Pelita Bangsa dan para dosen pembimbing atas segala dukungan dan bimbingan selama proses penelitian. Terima kasih juga kepada pihak perusahaan yang telah memberikan akses dan informasi yang diperlukan sesuai kesepakatan kerahasiaan yang berlaku.

KONFLIK KEPENTINGAN

Para penulis menyatakan bahwa tidak terdapat konflik kepentingan dalam penelitian ini, baik antara para penulis maupun dengan objek penelitian yang diteliti.

DAFTAR PUSTAKA

[1] S. Sternad Zabukovšek, S. Jordan, and S. Bobek, “Managing Document Management Systems’ Life Cycle in Relation to an Organization’s Maturity for Digital Transformation,” *Sustainability*, vol. 15, no. 21, p. 15212, Oct. 2023, doi: 10.3390/su152115212.

[2] L. Xing, “Secure Official Document Management and intelligent Information Retrieval System based on recommendation algorithm,” *International Journal of Intelligent Networks*, vol. 5, pp. 110–119, 2024, doi: 10.1016/j.ijin.2024.02.003.

[3] Firoz Mohammed Ozman, “Systematic literature review on ‘secure document management systems (DMS),’” *World J. Adv. Eng. Technol. Sci.*, vol. 15, no. 1, pp. 1460–1469, Apr. 2025, doi: 10.30574/wjaets.2025.15.1.0146.

[4] Badan Siber dan Sandi Negara Republik Indonesia, "Lanskap Keamanan Siber Indonesia 2023." Accessed: Mar. 05, 2026. [Online]. Available: https://bssn.go.id/laporan-keamanan-siber-indonesia/

[5] S. Bag, S. Sarkar, and I. Bose, "Enhancing cybersecurity risk assessment using temporal knowledge graph-based explainable decision support system," *Decision Support Systems*, vol. 198, p. 114526, Nov. 2025, doi: 10.1016/j.dss.2025.114526.

[6] F. A. Shaikh and M. Siponen, "Information security risk assessments following cybersecurity breaches: The mediating *role* of top management attention to cybersecurity," *Computers & Security*, vol. 124, p. 102974, Jan. 2023, doi: 10.1016/j.cose.2022.102974.

[7] OWASP Top 10 Team, "OWASP Top 10:2021. The Ten Most Critical Web Application Security Risks," OWASP Foundation. Accessed: Jan. 04, 2026. [Online]. Available: https://owasp.org/Top10/2021/

[8] OWASP Top 10 Team, "OWASP Top 10:2025, Application Security Risks," OWASP Foundation. Accessed: Jan. 04, 2026. [Online]. Available: https://owasp.org/Top10/

[9] N. A. Chandra, K. Ramli, A. A. P. Ratna, and T. S. Gunawan, "Information Security Risk Assessment Using Situational Awareness *Framework*s and Application Tools," *Risks*, vol. 10, no. 8, p. 165, Aug. 2022, doi: 10.3390/risks10080165.

[10] D. E. R. Hidayatullah, R. Kunthi, and R. Harwahyu, "Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department," *IJECBE*, vol. 2, no. 3, Sep. 2024, doi: 10.62146/ijecbe.v2i3.81.

[11] M. N. Irfan, S. Ramadhania, S. Hadi, and P. T. Pungkasanti, "ISO/IEC 27005-Based *E-Learning* Risk Management with *Blockchain* Architecture: A Case Study of Semarang University," *journalisi*, vol. 7, no. 3, pp. 2898–2919, Sep. 2025, doi: 10.51519/journalisi.v7i3.1265.

[12] M. L. B. Hikam, F. Dewi, and D. Praditya, "Analisis Manajemen Risiko Informasi Menggunakan Iso/Iec 27005:2018 (Studi Kasus: PT.XYZ)," *jipi. jurnal. ilmiah. penelitian. dan. pembelajaran. informatika.*, vol. 9, no. 2, pp. 728–734, May 2024, doi: 10.29100/jipi.v9i2.4709.

[13] N. Chandra and M. Yusuf, "Penilaian Resiko Keamanan Aplikasi Web Menggunakan Standar Iso/Iec 27005:2022 Pada Layanan Organisasi: Penilaian Resiko Keamanan Aplikasi Web Menggunakan Standar Iso/Iec 27005:2022 Pada Layanan Organisasi," *CoSciTech*, vol. 6, no. 2, pp. 206–213, Sep. 2025, doi: 10.37859/coscitech.v6i2.9994.

[14] I. O. for S. (ISO) International Electrotechnical Commission (IEC), "ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection, Information security, management systems Requirements." ISO/IEC, Geneva, Switzerland, Oct. 2022. Accessed: Jan. 06, 2026. [Online]. Available: https://www.iso.org/standard/27001

[15] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "ISO/IEC 27005:2022 , Information security, cybersecurity and privacy protection. Guidance on managing information security risks." ISO/IEC, Geneva, Switzerland, Oct. 2022. Accessed: Jan. 06, 2026. [Online]. Available: https://www.iso.org/standard/80585.html

[16] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," *Sustainability*, vol. 15, no. 7, p. 5828, Mar. 2023, doi: 10.3390/su15075828.

[17] A. P. Putra and B. Soewito, "Integrated Methodo*log*y for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector," *IJACSA*, vol. 14, no. 4, 2023, doi: 10.14569/IJACSA.2023.0140468.

[18] M. S. Sahira, R. Indriati, and A. Ristyawan, "Analisis Risiko *Website* Sistem Keamanan Informasi Menggunakan Metode Fmea dan *Framework* ISO/IEC 27002:2022," *J. Sist. Inform. Tek. Inform. Komput.*, vol. 3, no. 2, pp. 128–138, Jun. 2025, doi: 10.53624/jsitik.v3i2.722.

[19] P. Jatkiewicz, "Assessing cybersecurity methodo*log*ies: integrating competitiveness factor for risk analysis and IT system design," *Expert Systems with Applications*, vol. 296, p. 129220, Jan. 2026, doi: 10.1016/j.eswa.2025.129220.

[20] H. Artajaya, Julieta, J. Giancarlos, J. V. Moniaga, and A. Chowanda, "Development of a Secure Web Based Application to Automate Data Synchronization and Processing," *Procedia Computer Science*, vol. 245, pp. 1175–1181, 2024, doi: 10.1016/j.procs.2024.10.347.

[21] J. Rice and N. Martin, "Managing cybersecurity risks in Small businesses: A simulation-based decision *framework*," *Technological Forecasting and Social Change*, vol. 223, p. 124456, Feb. 2026, doi: 10.1016/j.techfore.2025.124456.

[22] G. Breda and M. Kiss, "Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security," *Procedia Manufacturing*, vol. 46, pp. 580–590, 2020, doi: 10.1016/j.promfg.2020.03.084.

[23] M. Fahrurozi, S. A. Tarigan, M. Alam Tanjung, and K. Mutijarsa, "The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence)," in *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, Yogyakarta, Indonesia: IEEE, Oct. 2020, pp. 86–91. doi: 10.1109/ICITEE49829.2020.9271748.

[24] F. Casarosa, G. Comandé, and J. Fortuna, "Proposing ELDA methodo*log*y: Ethical and Legal by Design and Assessment for cybersecurity solutions," *Computer Law & Security Review*, vol. 59, p. 106220, Nov. 2025, doi: 10.1016/j.clsr.2025.106220.

[25] H. M. Melaku, "Context-Based and Adaptive Cybersecurity Risk Management *Framework*," *Risks*, vol. 11, no. 6, p. 101, May 2023, doi: 10.3390/risks11060101.