NIVEDITA JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)

Vol. 01, No. 2, Juni 2025

ANALISIS RISIKO KEAMANAN SISTEM INFORMASI MENGGUNAKAN ISO 27005 PADA INSTANSI XYZ

M. Irvan[1], MHD. Agung Rizaldy[2], Megawati[3]

[1,2,3]Prodi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Sultan Syarif Kasim Riau, Indonesia

email: 12150313710@students.uin-suska.ac.id

Abstract

The public service application at XYZ Agency is a system used to support infrastructure and communication management and the provision of public services. However, this system faces various information security risks, such as data leakage and operational disruption threats. This research aims to conduct a risk assessment of possible threats using the ISO 27005 standard. The results showed that of the 13 risk scenarios identified, 12 risks were at a moderate level, while the highest risk was server down. Risk handling strategies include risk modification (RM) for most scenarios, as well as a combination of other strategies such as risk avoidance (RA) and risk sharing (RS). Suggestions for risk mitigation include the implementation of controls such as information backup (A.12.3.1) through regular data backups, both local and cloud, controls against malware (A.12.2.1) for the prevention of malicious software, and equipment maintenance (A.11.2.4) to ensure hardware continues to function optimally. This research concludes that ISO 27005 is the right standard to identify, assess and manage information security risks.

Keywords: *ISO 27005, Information Security, Risk Mitigation, Public Service Applications, Risk Assessment.*

Abstrak

Aplikasi pelayanan masyarakat di Instansi XYZ merupakan sistem yang digunakan untuk mendukung pengelolaan infrastruktur dan komunikasi serta penyediaan layanan publik. Namun, sistem ini menghadapi berbagai risiko keamanan informasi, seperti kebocoran data dan ancaman gangguan operasional. Penelitian ini bermaksud untuk melaksanakan penghitungan risiko terhadap kemungkinan ancaman dengan mengaplikasikan standar ISO 27005. Hasil penelitian menunjukkan bahwa dari 13 skenario risiko yang diidentifikasi, 12 risiko berada pada tingkat sedang, sementara risiko tertinggi adalah server down. Strategi penanganan risiko meliputi risk modification (RM) untuk sebagian besar skenario, serta kombinasi strategi lain seperti *risk avoidance* (RA) dan *risk sharing* (RS). Saran untuk mitigasi risiko termasuk penerapan kontrol seperti *information backup* (A.12.3.1) melalui pencadangan data secara berkala, baik server lokal maupun *online* , *controls against malware* (A.12.2.1) untuk pencegahan perangkat lunak berbahaya, dan *equipment maintenance* (A.11.2.4) untuk memastikan *hardware* tetap berfungsi optimal. Penelitian ini menyimpulkan bahwa ISO 27005 adalah standar yang tepat untuk mengidentifikasi, menilai, dan mengelola risiko keamanan informasi.

Kata kunci: ISO 27005, Keamanan Informasi, Mitigasi Risiko, Aplikasi Pelayanan Masyarakat, Penilaian Risiko

Diajukan: 26 Desember 2024; Direvisi: 19 April 2025; Diterima: 1 Juni 2025

PENDAHULUAN

Sistem informasi saat ini tidak hanya digunakan di dunia bisnis, tetapi juga digunakan di berbagai bidang, termasuk pendidikan, pemerintahan, industri, dan masih banyak lagi[1]. Instansi XYZ merupakan salah satu bidang pemerintahan yang berwenang untuk mengatur sarana dan prasarana teknologi informasi dan komunikasi daerah, sangat bergantung pada integritas, ketersediaan, dan kerahasiaan data serta sistem informasi yang dikelola[2]. Namun sistem informasi sering menghadapi risiko ancaman keamanan sistem informasi.

Risiko merupakan sebuah ketidakpastian yang bisa menghambat organisasi untuk mencapai tujuan bisnis [3]. Risiko dipengaruhi oleh *Risk Driver* dan *Risk Control*, dimana *Risk Drivers* merupakan faktor yang meningkatkan ketidakpastian[4]. Ketika sistem informasi terancam, proses sistem akan terganggu, terutama dalam hal keamanan data dan informasi[5]. Ancaman serangan seperti *malware*, peretasan

NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025

(*hacking*), dan kebocoran data (*data breaches*) telah menjadi isu yang semakin mendesak bagi instansi pemerintah. Sangat penting untuk mengelola risiko keamanan informasi untuk memastikan sistem informasi institusi pemerintah aman karena gangguan dapat mengganggu pelayanan publik dan menghilangkan kepercayaan masyarakat terhadap pemerintah. Analisis risiko keamanan bertujuan untuk mengidentifikasi berbagai ancaman dan potensi risiko. Kajian terkait pengelolaan keamanan informasi diterapkan untuk menjaga sumber daya dalam sistem dari ancaman seperti kebocoran data serta untuk mencegah akses berizin masuk ke dalam sistem informasi.

ISO 27005 merupakan salah satu kerangka kerja dalam mengevaluasi dan menganalisa tingkat risiko keamanan sistem informasi[6]. ISO 27005 merupakan prosedur sistematis yang dirancang untuk mengelola risiko keamanan sistem informasi. Standar ini membantu menentukan kebutuhan organisasi dalam menjaga keamanan informasi serta membangun Sistem Manajemen Keamanan Informasi (SMKI) yang efektif. Berdasarkan penelitian hikam (2024) dengan menggunakan kerangka kerja ISO 27005, perusahaan dapat memastikan bahwa ancaman terhadap aset informasi mereka diidentifikasi secara tepat dan dikendalikan dengan langkah yang terstruktur [7].

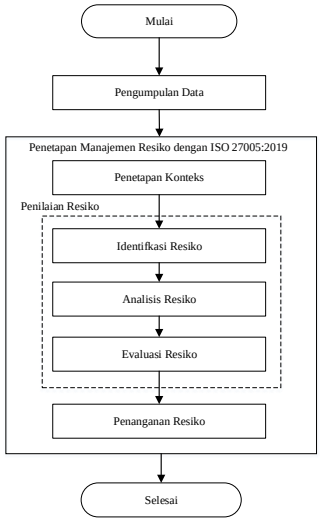
ISO 27005 sebuah standar yang memberikan panduan terperinci dalam pengelolaan risiko keamanan informasi. Standar ini dirancang untuk membantu individu atau organisasi dalam merumuskan strategi pengelolaan keamanan informasi yang efektif. Prosesnya dimulai dengan langkah identifikasi risiko, yang memungkinkan organisasi mengenali potensi ancaman dan kerentanan terhadap sistem informasi mereka. Setelah risiko berhasil diidentifikasi, dilakukan analisis mendalam untuk menentukan langkah-langkah penanganan atau mitigasi yang tepat guna mengurangi dampak yang mungkin terjadi. ISO 27005 dipilih sebagai kerangka acuan karena dianggap menyediakan pendekatan yang lebih mudah dan sistematis dalam mengelola keamanan informasi, sehingga organisasi dapat lebih efisien dalam melindungi aset informasi mereka dari berbagai ancaman yang ada. [8].

Adanya risiko manejemen keamanan sistem informasi maka diperlukan evaluasi dan analisa terhadap risiko tersebut untuk mengetahui ancaman risiko yang terjadi dan mengetahui tingkat risiko keamanan sistem informasi. Berdasarkan penelitian yang dilakukan oleh Sahira dan Leasa, Penerapan analisis keamanan sistem informasi menggunakan standar ISO 27005 bertujuan untuk mengelola risiko keamanan sistem informasi secara efektif, setiap ancaman yang mungkin terjadi dapat ditangani secara optimal dan menjadi bahan pertimbangan saat mengembangkan sistem informasi.[9], [10].

Dengan demikian, penelitian ini tidak hanya relevan dalam konteks peningkatan keamanan sistem informasi di Instansi XYZ, tetapi juga diharapkan dapat menyumbangkan partisipasi yang signifikan dalam pengembangan kebijakan keamanan informasi risiko di lingkungan pemerintahan daerah.

METODE

Dalam sistem informasi milik instansi XYZ, analisis risiko keamanan informasi dilakukan dengan menerapkan standar ISO 27005. Standar internasional ini memberikan panduan untuk mengelola risiko keamanan informasi secara sistematis [11]. Pendekatan ini harus disesuaikan dengan karakteristik lingkungan perusahaan serta terintegrasi dengan kerangka manajemen risiko perusahaan secara keseluruhan [12]. Data untuk penelitian ini diperoleh melalui konsultasi dengan pihak yang bertanggung jawab atas manajemen sistem informasi. Proses penelitian yang dilakukan dirangkum dalam langkah-langkah yang ditunjukkan pada Gambar 1.



Gambar 1. Metodologi penelitian

Proses ini dimulai dengan penentuan strategi dan prosedur untuk mengelola risiko keamanan informasi. Langkah pertama mencakup pengumpulan data, yang dilakukan melalui wawancara, observasi, dan penelitian pustaka. Data ini memberikan gambaran tentang keadaan sistem informasi, aset yang dimiliki, potensi ancaman, dan kontrol keamanan yang telah diterapkan.

Selanjutnya, proses dimulai dengan penetapan sistem manajemen risiko. Pada titik ini, penetapan konteks dilakukan untuk menentukan jangkauan analisis. Peneliti menemukan sumber daya penting sistem, memahami prosedur bisnis yang mendukungnya, dan menyesuaikan tujuan analisis risiko dengan standar yang telah ditentukan. Penetapan konteks ini menjamin bahwa semua bagian yang berpartisipasi dalam tindakan manajemen risiko memiliki pengetahuan yang sama tentang arah dan tujuan proses tersebut.

Penilaian risiko adalah bagian krusial dari pengelolaan risiko, yang mencakup tiga langkah utama yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko. Identifikasi risiko mencakup pendataan aset, ancaman, kelemahan, dan kontrol yang ada untuk mengidentifikasi sumber-sumber risiko. Selanjutnya, risiko yang telah diidentifikasi dianalisis berdasarkan kemungkinan terjadi dan efeknya terhadap sistem, sehingga tingkat risiko dapat ditentukan. Untuk membantu pengambilan keputusan, tahap evaluasi risiko menghasilkan daftar risiko yang dikategorikan berdasarkan tingkatannya, seperti rendah, sedang, atau tinggi.

Penanganan risiko dilakukan setelah penilaian risiko selesai. Mengalihkan risiko kepada pihak ketiga, seperti penyedia asuransi, atau meningkatkan kontrol keamanan untuk mengurangi risiko, menerima risiko tertentu yang dianggap dapat ditoleransi, atau menghindari aktivitas berisiko untuk menghilangkan risiko sepenuhnya adalah beberapa strategi yang dapat digunakan. Tujuan dari tindakan ini adalah untuk membenarkan bahwa risiko yang teridentifikasi dapat dikurangi atau dikelola dengan cara yang paling efisien.

Proses ini diakhiri dengan penerapan langkah-langkah mitigasi yang direkomendasikan, sehingga sistem informasi lebih terlindungi dari potensi ancaman. Alur ini menggambarkan pendekatan sistematis dalam mengelola risiko keamanan informasi, dimulai dari pengumpulan data hingga penanganan risiko, sesuai dengan pedoman ISO 27005.

HASIL DAN PEMBAHASAN

Dalam penelitian ini, kerangka kerja yang digunakan yaitu ISO 27005 untuk manajemen risiko keamanan sistem informasi di instansi pemerintah XYZ. Proses penilaian risiko dimulai dengan identifikasi dan kemudian melakukan analisis risiko yang mungkin terjadi untuk menghasilkan hasil yang dibutuhkan dalam proses evaluasi.

Penetapan Konteks

Langkah manajemen risiko yang dilaksanakan dalam penelitian ini berasal dari kerangka kerja ISO 27005, dengan ruang lingkup studi yang mencakup tiga fase, yaitu penetapan konteks, penilaian risiko, dan penanganan risiko. Setiap tahapan dirancang secara terstruktur untuk memastikan setiap potensi risiko keamanan informasi dapat diidentifikasi, dianalisis, dan ditangani secara efektif sesuai dengan prinsip-prinsip standar ISO 27005.

Penilaian Risiko

Proses penilaian risiko keamanan sistem informasi di instansi XYZ melibatkan tiga tahap utama yang saling berkesinambungan. Tahap pertama adalah identifikasi risiko, di mana potensi ancaman terhadap sistem informasi diidentifikasi secara rinci. Selanjutnya, tahap analisis risiko yang bertujuan untuk memahami tingkat keparahan dan dampak dari setiap risiko yang teridentifikasi. Terakhir, tahap evaluasi risiko bertujuan untuk menilai prioritas risiko dan menentukan langkah mitigasi yang sesuai guna mengurangi dampaknya terhadap keamanan sistem informasi.

Identifikasi Risiko

Proses identifikasi risiko dalam penelitian ini terdiri dari beberapa prosedur utama yang dirancang secara teratur sesuai dengan kerangka kerja ISO 27005. Langkah pertama adalah identifikasi aset, di mana aset informasi yang perlu dilindungi diidentifikasi dan dipetakan. Selanjutnya, dilakukan identifikasi ancaman untuk mengenali potensi sumber risiko yang dapat mengganggu keamanan aset tersebut. Proses ini diikuti dengan identifikasi kontrol yang ada (existing controls), yaitu langkah untuk menginventarisasi mekanisme perlindungan atau pengendalian yang sudah diterapkan. Terakhir, dilakukan identifikasi kerentanan (vulnerabilities) guna mengungkap titik lemah yang dapat dieksploitasi oleh ancaman.

NIVEDITA JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025

Pendekatan ini memastikan bahwa seluruh aspek risiko keamanan informasi teridentifikasi secara komprehensif dan terstruktur.

Pada tahap identifikasi aset, fokus diberikan pada aset-aset yang dimiliki oleh Instansi XYZ dalam operasional aplikasi Pelayanan. Aset-aset tersebut diklasifikasikan ke dalam dua kategori utama:

1. Aset Utama: Aplikasi pelayanan, yang menjadi pusat aktivitas operasional dan penyediaan layanan kepada pengguna.
2. Aset Pendukung: Infrastruktur teknologi dan perangkat seperti perangkat keras (*hardware*) dan perangkat lunak (*software*), yang mendukung operasional aplikasi tersebut

Identifikasi yang terperinci ini bertujuan untuk memahami secara komprehensif elemen-elemen yang harus dilindungi serta hubungan antara aset utama dan pendukung, sehingga dapat mempermudah proses analisis ancaman dan kerentanan dalam tahapan berikutnya.

Identifikasi ancaman pada aset teknologi informasi yang dimiliki instansi XYZ, risiko dapat bersumber dari alam dan kelalaian pengguna yang disajikan pada Tabel 1. dengan kode PK melambangkan aset perangkat keras dan kode PL untuk aset perangkat lunak.

Tabel 1. Identifikasi aset dan ancaman

No	Aset	Kode	Ancaman
1.	Perangkat Keras	PK1	Kebakaran
		PK2	Bencana Alam
		PK3	Pemadaman Listrik
		PK4	Koneksi Jaringan Terputus
		PK5	Kegagalan/ Rusaknya Hardware
		PK6	Kesalahan Pengguna
		PK7	Server Down
2.	Perangkat Lunak	PL1	Akses Data oleh Pihak yang tidak Berwenang
		PL2	Serangan Virus
		PL3	Kesalahan Pengguna
		PL4	Login Secara Paksa
		PL5	Serangan DDoS
		PL6	Kebocoran dan Hilangnya Data

Tabel 1. Menyajikan hasil identifikasi risiko yang mencakup berbagai ancaman potensial terhadap sistem informasi. Ancaman-ancaman ini dikategorikan ke dalam dua jenis utama, yaitu ancaman alam (seperti bencana alam) dan ancaman manusia (seperti kesalahan pengguna atau serangan siber). Untuk mempermudah proses identifikasi dan analisis risiko di tahap selanjutnya, setiap ancaman diberi kode khusus yang terhubung dengan aset yang dimiliki.

Tabel 2. Berisi hasil identifikasi kontrol yang ada dan kerentanan yang terkait dengan aset. Identifikasi kontrol yang ada bertujuan untuk mengevaluasi mekanisme perlindungan yang telah diterapkan pada aset, dengan fokus pada efisiensi untuk mencegah pengeluaran biaya yang tidak perlu. Sementara itu, identifikasi kerentanan mencakup penilaian terhadap titik lemah pada aset yang dapat dimanfaatkan oleh ancaman. Kedua tabel ini memberikan landasan untuk pengembangan strategi mitigasi risiko yang lebih efektif.

Tabel 2. Identifikasi kontrol dan kerentanan

No	Aset	Kontrol yang ada	Kerentanan
1.	Perangkat Keras	Menyediakan alat pemadam kebakaran	Kurangnya kewaspadaan dalam menggunakan api di sekitar area kantor.
		Mempersiapkan Lokasi dengan memperhatikan aspek keamanannya	Bencana alam
		Menyediakan pembangkit Listrik cadangan	Listrik yang tidak stabil

NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025

No	Aset	Kontrol yang ada	Kerentanan
		Perbaikan atau menghubungi pihak ketiga	Koneksi Jaringan yang tidak stabil
		Melakukan pengecekan perangkat secara berkala	Kurangnya maintenance perangkat keras
		Edukasi penggunaan perangkat	Kurangnya pengetahuan pengguna
		Melakukan pemeliharaan secara berkala	Server menerima banyak permintaan
2.	Perangkat Lunak	Melakukan verifikasi	Mengubah data tanpa izin
		Memperbarui antivirus secara berkala	Gangguan pada layanan yang disebabkan oleh virus yang tidak terdeteksi
		Edukasi penggunaan perangkat lunak	Kurangnya pengetahuan penggunaan perangkat lunak
		Akses diberikan kepada pengguna yang berhak	Tidak ada Batasan hak akses
		Meningkatkan keamanan sistem informasi	Meningkatnya lalu lintas jaringan internet
		Terapkan prosedur backup yang otomatis dan terjadwal.	Celah keamanan dalam aplikasi yang memungkinkan akses ilegal ke data.

Tabel 2 memuat informasi mengenai identifikasi kontrol yang ada (*existing controls*) serta kerentanan (*vulnerabilities*) yang terkait dengan aset yang dimiliki oleh instansi XYZ. Kontrol yang ada menggambarkan langkah-langkah atau mekanisme perlindungan yang diterapkan untuk menghadapi ancaman atau mengurangi dampak kerentanan yang muncul dalam aktivitas operasional saat ini. Sementara itu, kerentanan mencakup titik lemah atau risiko yang dapat muncul pada berbagai kegiatan atau proses yang bergantung pada aset organisasi.

Dalam konteks perangkat keras dan perangkat lunak, kerentanan yang paling signifikan ditemukan pada aplikasi layanan masyarakat, yang menjadi fokus utama. Hal ini dikarenakan aplikasi tersebut merupakan elemen vital dalam mendukung layanan publik, sehingga rentan terhadap ancaman teknis maupun nonteknis. Identifikasi ini bertujuan untuk memastikan bahwa langkah pengendalian yang diterapkan mampu melindungi aset-aset kritis organisasi secara optimal.

Analisis Risiko

Pada tahap ini akan dilakukan evaluasi terhadap risiko yang telah diidentifikasi sebelumnya. Kemungkinan risiko dan kategori dampak terjadinya risiko akan digunakan untuk menentukan nilai ini. Dengan tingkatan kemungkinan risiko diawali dari sangat tidak mungkin (1), tidak mungkin (2), mungkin (3), besar kemungkinan (4) dan sering (5), dengan nilai tingkatan mulai dari 1 sampai 5. Tingkat dampak terjadinya risiko mulai dari dampak yang tidak berpengaruh hingga dampak yang sangat berpengaruh dan memunculkan gangguan pada pelayanan. Tingkatan dari akibat ancaman risiko, mulai dari sangat rendah (1), rendah (2), sedang (3), tinggi (4) dan sangat tinggi (5), dengan tingkat dampak yang berkisar dari sangat rendah (nilai 1) hingga sangat tinggi (nilai 5), analisis risiko berikut ini didasarkan pada penilaian nilai ancaman dan dampaknya., dapat dilihat pada tabel 3. di bawah ini

Tabel 3. Analisis risiko

No	Aset	Kontrol yang ada	Kerentanan	Nilai Ancaman	Nilai Dampak
1.	Perangkat Keras	Menyediakan alat pemadam kebakaran	Kurangnya kewaspadaan dalam menggunakan api di sekitar area kantor.	Tidak mungkin	Sedang
		Mempersiapkan Lokasi dengan memperhatikan aspek keamanannya	Bencana alam	Tidak mungkin	Tinggi
		Menyediakan pembangkit Listrik cadangan	Listrik yang tidak stabil	Mungkin	Sedang

NIVEDITA JOURNAL INFORMATICS
ISSN 3089-8366 (Media Online)
Vol. 01, No. 2, Juni 2025

No	Aset	Kontrol yang ada	Kerentanan	Nilai Ancaman	Nilai Dampak
		Perbaikan atau menghubungi pihak ketiga	Koneksi Jaringan yang tidak stabil	Besar kemungkinan	Sedang
		Melakukan pengecekan perangkat secara berkala	Kurangnya maintenance perangkat keras	Tidak mungkin	Sedang
		Edukasi penggunaan perangkat	Kurangnya pengetahuan pengguna	Tidak mungkin	Sedang
		Melakukan pemeliharaan secara berkala	Server menerima banyak permintaan	Besar kemungkinan	Sangat Tinggi
2.	Perangkat Lunak	Melakukan verifikasi	Mengubah data tanpa izin	Tidak mungkin	Sedang
		Memperbarui antivirus secara berkala	Gangguan pada layanan yang disebabkan oleh virus yang tidak terdeteksi	Mungkin	Sedang
		Edukasi penggunaan perangkat lunak	Kurangnya pengetahuan penggunaan perangkat lunak	Mungkin	Tinggi
		Akses diberikan kepada pengguna yang berhak	Tidak ada Batasan hak akses	Mungkin	Tinggi
		Meningkatkan keamanan sistem informasi	Meningkatnya lalu lintas jaringan internet	Mungkin	Tinggi
		Terapkan prosedur backup yang otomatis dan terjadwal.	Celah keamanan dalam aplikasi yang memungkinkan akses ilegal ke data.	Mungkin	Rendah

Dalam analisis risiko ini, penilaian dilakukan berdasarkan dua pendekatan, yaitu kualitatif dan kuantitatif. Penilaian kualitatif mempertimbangkan potensi ancaman dan risiko secara deskriptif, dengan fokus pada analisis mendalam terhadap kemungkinan dampak dari ancaman tersebut. Sebaliknya, dalam pendekatan kuantitatif, hasil analisis risiko diekspresikan dalam bentuk angka. Penilaian kuantitatif dilakukan dengan menghitung nilai risiko yang diperoleh dari perhitungan antara nilai peluang terjadinya ancaman dan nilai dampaknya. Berdasarkan matriks penilaian risiko, tingkat risiko dikelompokkan menjadi beberapa golongan utama yaitu risiko rendah dengan kemungkinan dan dampak minimal, risiko sedang dengan kemungkinan atau dampak yang menengah dan risiko tinggi dengan kemungkinan dan dampak yang signifikan.

Setelah analisis risiko dilakukan, dibuat daftar prioritas risiko untuk membantu menentukan langkah mitigasi yang tepat. Daftar ini disusun berdasarkan nilai risiko yang diidentifikasi sebelumnya, dengan hasil penilaian disajikan secara rinci dalam Tabel 4. Tabel ini menjadi panduan untuk memfokuskan sumber daya pada pengelolaan risiko dengan tingkat prioritas tertinggi.

Tabel 4. Hasil penilaian risiko

No	Kode	Nilai Ancaman	Nilai Dampak	Nilai Risiko	Level Risiko
1.	PK1	2	3	6	Sedang
	PK2	2	4	8	Sedang
	PK3	3	3	9	Sedang
	PK4	4	3	12	Sedang
	PK5	2	3	6	Sedang
	PK6	2	3	6	Sedang
	PK7	4	5	20	Sangat Tinggi
2.	PL1	2	3	6	Sedang
	PL2	3	3	9	Sedang

NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 2, Juni 2025

No	Kode	Nilai Ancaman	Nilai Dampak	Nilai Risiko	Level Risiko
	PL3	3	4	12	Sedang
	PL4	3	4	12	Sedang
	PL5	3	4	12	Sedang
	PL6	3	2	6	Sedang

Berdasarkan Tabel 4. Hasil penilaian tingkat risiko menunjukkan rata-rata berada pada level risiko sedang. Namun, dari berbagai ancaman yang teridentifikasi, ancaman tertinggi terdapat pada kode aset PK7, yaitu ketika terjadi server down..

Evaluasi Risiko

Pada proses ini, hal pertama yang dikerjakan adalah membuat matriks penilaian risiko yang didasarkan pada hubungan antara nilai ancaman dan nilai dampak. Harapan dari matriks ini ialah untuk menemukan dan menvisualisasikan tingkat risiko berdasarkan kombinasi kedua parameter tersebut. Tabel 5. Menunjukkan secara rinci hubungan antara tingkat ancaman dan dampak terhadap aset teknologi informasi, sehingga memudahkan dalam menentukan prioritas mitigasi risiko.

Tabel 5. Matrik penilaian risiko

		Nilai Ancaman				
		1	**2**	**3**	**4**	**5**
Nilai Dampak	**1**					
	2		PL6			
	3		PK1,PK5,PK6,PL1	PK3,PL2	PK4	
	4		PK2	PL3,PL4,PL5		
	5				PK7	

Risiko dikategorikan berdasarkan tingkat keparahan dan kemungkinan terjadinya. Risiko rendah (hijau) memiliki dampak kecil dan kemungkinan rendah, memerlukan pengawasan minimal. Risiko sedang (kuning) berdampak cukup signifikan atau kemungkinan sedang, membutuhkan mitigasi lebih serius. Risiko tinggi (merah) berdampak besar atau sangat mungkin terjadi, memerlukan tindakan segera dan pengelolaan intensif.

Berdasarkan tabel 5. Diatas hasil dari proses pembuatan matrik penilaian risiko menunjukkan bahwa rata rata tingkat risiko berada pada level sedang, selain itu terdapat juga risiko yang berada di level tinggi yaitu *server down*. Daftar level risiko atau ancaman yang berpotensi terjadi dapat dilihat pada tabel 6. Berikut.

Tabel 6. Daftar level risiko

Level risiko	Kode
Rendah	
Sedang	PK1,PK2,PK3,PK4,PK5,PK6,PL1,PL2,PL3,PL4,PL5,PL6
Tinggi	PK7

Penanganan Risiko

Pada tahap ini,, proses pengambilan keputusan terkait tindakan penanganan risiko dilakukan didasari oleh hasil analisis terhadap tingkat kemungkinan dan akibat dari setiap ancaman yang teridentifikasi. Tindakan penanganan risiko ini terbagi ke dalam empat strategi utama, yaitu: modifikasi risiko (*Risk Modification/RM*), mempertahankan risiko (*Risk Retention/RR*), menghindari risiko (*Risk Avoidance/RA*), dan membagi risiko (*Risk Sharing/RS*).

a) Modifikasi risiko (*Risk Modification*) dilakukan dengan tujuan mengurangi tingkat kemungkinan terjadinya ancaman atau menurunkan dampaknya melalui perubahan pada sistem, proses, atau prosedur yang ada.
b) Mempertahankan risiko (*Risk Retention*) merupakan pendekatan untuk menerima dan menanggung risiko tertentu jika dianggap kecil atau jika biaya mitigasi melebihi potensi kerugian.
c) Menghindari risiko (*Risk Avoidance*) melibatkan penghapusan sepenuhnya terhadap potensi risiko dengan cara menghindari aktivitas atau keputusan yang dapat memicu ancaman.

d) Membagi risiko (*Risk Sharing*) dilakukan dengan mengalihkan sebagian atau seluruh risiko kepada pihak ketiga, seperti melalui asuransi atau kerja sama dengan penyedia layanan.

Hasil dari penilaian risiko yang mencakup identifikasi ancaman, penentuan tingkat risiko, dan pemilihan strategi penanganannya, disajikan secara sistematis pada Tabel 7. Penyajian ini digunakan untuk menyajikan pemahaman yang menyeluruh terkait prioritas mitigasi risiko, alokasi sumber daya, serta langkah-langkah strategis yang perlu diambil untuk memastikan keberlanjutan operasional sistem dan organisasi.

Tabel 7. Hasil penilaian risiko

Kode	Level Risiko	Biaya pemulihan	Penanganan Risiko	Keterangan
PK1	Sedang	Sedang	RM	Menyediakan alat pemadam kebakaran
PK2	Sedang	Tinggi	RM	Mempersiapkan Lokasi dengan memperhatikan aspek keamanannya
PK3	Sedang	Rendah	RM	Menyediakan pembangkit Listrik cadangan
PK4	Sedang	Sedang	RS	Perbaikan atau menghubungi pihak ketiga
PK5	Sedang	Tinggi	RM	Melakukan pengecekan perangkat secara berkala
PK6	Sedang	Sedang	RM	Edukasi penggunaan perangkat
PK7	Tinggi	Tinggi	RA	Melakukan pemeliharaan secara berkala
PL1	Sedang	Sedang	RA	Melakukan verifikasi
PL2	Sedang	Sedang	RR	Memperbarui antivirus secara berkala
PL3	Sedang	Tinggi	RA	Edukasi penggunaan perangkat lunak
PL4	Sedang	Rendah	RA	Akses diberikan kepada pengguna yang berhak
PL5	Sedang	Tinggi	RA	Meningkatkan keamanan sistem informasi
PL6	Sedang	Tinggi	RM	Terapkan prosedur backup yang otomatis dan terjadwal.

Hasil dari mitigasi ini umumnya berada pada *risk modification* (RM). Namun untuk kode aset PK7 mendapat level risiko tinggi dengan biaya perbaikan tinggi, maka untuk penanganan risiko yang dilakukan yaitu *risk avoidance* (RA).

Berlandaskan pada hasil analisis penilaian risiko yang terdapat pada Tabel 7. Maka saran yang cocok untuk mengatasi risiko pada keamanan sistem informasi aplikasi pelayanan masyarakat menggunakan ISO 27005 yaitu:

1. Tindakan Pengelolaan kode PK1 dan PK2 yaitu *equipment sitting and protection* (A.11.2.1) dengan menyediakan peralatan untuk melindungi setiap aset dari ancaman.
2. Tindakan Pengelolaan pada kode PK3 dan PK4 yaitu *supporting utilities* (A.11.2.2) dengan menggunakan pembangkit listrik cadangan dan memperbarui perangkat yang sudah usang.
3. Tindakan Pengelolaan kode PK5 yaitu *equipment maintenance* (A.11.2.4) dengan memelihara perangkat keras secara berkala.
4. Tindakan Pengelolaanl kode PK6 dan kode PL3 yaitu *management responsibilities* (A.7.2.1) dengan mengajarkan pengguna bagaimana menggunakan sistem informasi dengan tepat.
5. Tindakan Pengelolaan kode PL2 yaitu *controls against malware* (A.12.2.1) dengan meminimalisir dan melacak perangkat lunak yang memiliki potensi kerugian.
6. Tindakan Pengelolaan PL5 yaitu *installation of software on operational systems* (A.12.5.1) dengan mengubah sistem operasi yang ada dan meningkatkan keamanan melalui pengunaan *firewall &* VPN.
7. Tindakan Pengelolaan kode PK7, PL1, PL4 dan PL6 yaitu *information backup* (A.12.3.1) dengan melakukan backup data secara berkala.

KESIMPULAN

Berdasarkan hasil analisis risiko keamanan sistem informasi pada aplikasi pelayanan masyarakat di Instansi XYZ dengan menggunakan standar ISO 27005, ditemukan 13 potensi risiko yang mungkin terjadi. Risiko tersebut meliputi dari 1 ancaman pada tingkat tinggi dan 12 risiko pada tingkat sedang. Untuk mitigasi risiko keamanan sistem informasi, direkomendasikan penerapan sejumlah kontrol sesuai dengan standar ISO 27005, antara lain: *Equipment Sitting and Protection (A.11.2.1), Supporting Utilities (A.11.2.2), Equipment Maintenance (A.11.2.4), Management Responsibilities (A.7.2.1), Controls Against Malware (A.12.2.1), Installation of Software on Operational Systems (A.12.5.1), serta Information Backup (A.12.3.1).*

Analisis risiko keamanan sistem informasi harus dilanjutkan pada aplikasi pelayanan masyarakat lainnya. Ini disarankan untuk melakukan studi lebih lanjut untuk mendapatkan pengetahuan yang lebih mendalam dan khusus mengenai potensi ancaman keamanan informasi di berbagai konteks aplikasi pelayanan publik.

DAFTAR PUSTAKA

[1] D. Ramdhana Prasetya, T. Domai, and L. Indah Mindarti, “ANALISIS PENGELOLAAN PENGADUAN MASYARAKAT DALAM RANGKA PELAYANAN PUBLIK (Studi Pada Dinas Komunikasi dan Informatika Kota Malang),” 2020.

[2] N. Afrina Prastiwi, S. Kholil, and S. Titin Sumanti, “PENGELOLAAN WEBSITE DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN ASAHAN SEBAGAI AKSES INFORMASI PUBLIK,” *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan*, vol. 1, no. 11, pp. 2605–2614, Oct. 2022, doi: 10.54443/sibatik.v1i11.399.

[3] K. Isnaini, G. J. Nofita Sari, and A. P. Kuncoro, “Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa,” *Jurnal Eksplora Informatika*, vol. 13, no. 1, pp. 37–45, Sep. 2023, doi: 10.30864/eksplora.v13i1.696.

[4] B. A. Nugraha, A. R. Perdanakusuma, and A. Rachmadi, “Analisa Manajemen Risiko pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800-30 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur,” 2020. [Online]. Available: http://j-ptiik.ub.ac.id

[5] K. Isnaini, G. J. Nofita Sari, and A. P. Kuncoro, “Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa,” *Jurnal Eksplora Informatika*, vol. 13, no. 1, pp. 37–45, Sep. 2023, doi: 10.30864/eksplora.v13i1.696.

[6] Syahindra P, Primasari C, and Irianto A, “EVALUASI RISIKO KEAMANAN INFORMASI DISKOMINFO PROVINSI XYZ MENGGUNAKAN INDEKS KAMI DAN ISO 27005 : 2011,” *JURNAL TEKNOINFO*, 2022.

[7] 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.

[8] S. Febyana, L. Fitriansyah, A. Kurniawan, and R. A. Nugroho, “Risk Management Analysis of Information Security in an Academic Information System at a Public University in Indonesia: Implementation of ISO/IEC 27005:2018 and ISO/IEC 27001:2013 Security Controls,” *Journal of Information Technology and Cyber Security*, vol. 2, no. 2, 2024, doi: 10.30996/jitcs.12099.

[9] S. Sahira, R. Fauzi, and I. Santosa, “ANALISIS MANAJEMEN RISIKO PADA APLIKASI E-OFFICE YANG DIKELOLA OLEH PT TELKOM INDONESIA MENGGUNAKAN STANDAR ISO/IEC 27005:2018 ANALYSIS OF RISK MANAGEMENT IN E-OFFICE APPLICATION MANAGED BY PT TELKOM INDONESIA USING ISO/IEC 27005:2018 STANDARD.”

[10] Z. V. Leasa and G. F. Prassida, “Manajemen Risiko pada Sistem Informasi Akademik Universitas XYZ menggunakan ISO 27005:2018,” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 6, no. 4, pp. 649–656, Oct. 2024, doi: 10.47233/jteksis.v6i4.1459.

[11] M. Amirinnisa1 and R. Bisma2, “Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun,” 2023.

[12] A. Ambarwati and C. Darujati, “Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005,” 2020. [Online]. Available: http://sistemasi.ftik.unisi.ac.id