Jurnal Informatika Ekonomi Bisnis

http://www.infeb.org

2025 Vol. 7 No. 2 Hal: 270-276 e-ISSN: 2714-8491

Penilaian Risiko Keamanan Informasi Pusat Data pada Instansi XYZ

Helsha Zania Artie[1]✉, Muhammad Hilman[2], Setiadi Yazid[3]

[1,2,3]Universitas Indonesia

helsha.zania31@ui.ac.id

Abstract

Information security is a critical aspect of protecting an organization's essential assets, including data centers that store and process sensitive information. The XYZ Agency, responsible for managing public finances, places a high priority on maintaining data confidentiality, integrity, and availability. Therefore, improving information security needs to be done through a risk assessment of assets located in the XYZ Agency Data Center. This research aims to evaluate information security risks at the XYZ Agency Data Center using the ISO 27005:2018 and NIST SP 800-30 frameworks. The assessment was performed through qualitative analysis involving interviews, internal document review, and observation. The findings revealed 111 identified risks, categorized as 48 very low risks, 50 low risks, 9 medium risks, and 4 high risks. Among these, 13 risks 4 high risks and 9 medium risks require mitigation. Mitigation efforts should prioritize seven data center assets with medium and high risks, namely application server assets, database servers, virtual host servers, agency service applications, agency service data, virtual server staffing applications, and staffing applications.

Keywords: Information Security, Risk Assessment, Data Center, ISO 27005, NIST SP 800-30.

Abstrak

Keamanan informasi merupakan aspek krusial dalam melindungi aset kritis organisasi, termasuk pada pusat data yang menyimpan dan memproses informasi sensitif. Instansi XYZ bertanggung jawab atas pengelolaan keuangan publik, sehingga keamanan informasi menjadi krusial untuk menjaga kerahasiaan, integritas, dan ketersediaan data. Oleh karena itu, peningkatan keamanan informasi perlu dilakukan melalui penilaian risiko terhadap aset yang berada pada Pusat Data Instansi XYZ. Penelitian ini bertujuan untuk menilai risiko keamanan informasi pada Pusat Data Instansi XYZ dengan menggunakan kerangka kerja ISO 27005:2018 dan NIST SP 800-30. Penilaian dilakukan melalui analisis kualitatif dengan metode wawancara, pengumpulan dokumen internal, serta observasi. Hasil penelitian menunjukkan terdapat 111 risiko yang teridentifikasi, terdiri atas 48 risiko sangat rendah, 50 risiko rendah, 9 risiko sedang, dan 4 risiko tinggi. Dari risiko tersebut 13 risiko yang terdiri dari 4 risiko tinggi dan 9 risiko sedang memerlukan mitigasi. Mitigasi dapat diprioritaskan pada tujuh aset pusat data yang memiliki risko sedang dan tinggi yaitu, aset server aplikasi, server database, server host virtual, aplikasi layanan instansi, data layanan instansi, server virtual aplikasi kepegawaian, dan aplikasi kepegawaian.

Kata kunci: Keamanan Informasi, Penilaian Risiko, Pusat Data, ISO 27005, NIST SP 800-30.

1. Pendahuluan

Keamanan informasi menjadi aspek yang sangat penting dalam melindungi aset kritis organisasi. Kebutuhan akan keamanan informasi semakin meningkat seiring dengan kompleksitas ancaman siber yang terus berkembang. Serangan siber kini lebih terorganisir, canggih, dan sering kali didukung dengan sumber daya yang besar. Laporan terbaru menunjukkan peningkatan serangan ransomware yang naik 41% dalam beberapa tahun terakhir [1]. Bahkan Halliburton, penyedia produk dan layanan global untuk industri energi mengungkapkan bahwa serangan ransomware yang terjadi pada bulan Agustus 2024 telah menyebabkan kerugian sebesar $35 juta setelah serangan tersebut menyebabkan perusahaan mematikan sistem TI dan memutuskan koneksi dengan pelanggan [2].

Dari kejadian tersebut dapat diketahui bahwa pentingnya keamanan informasi pada aset kritis yang dimiliki organisasi. Salah satu yang menjadi aset kritis dalam organisasi, adalah pusat data (*data center*) yang menyimpan dan memproses informasi sensitif. *Pusat data* adalah fasilitas yang menyediakan berbagai sumber daya untuk memproses, menyimpan, dan mendistribusikan informasi digital. Fasilitas ini mencakup perangkat teknologi informasi (TI) beserta infrastruktur pendukungnya, seperti sistem kelistrikan, pendinginan, telekomunikasi, perlindungan kebakaran, keamanan, dan sistem otomatisasi [3].

Instansi XYZ merupakan salah satu lembaga yang memiliki tanggungjawab yang besar dalam pengelolaan keuangan di sektor publik. Keamanan informasi menjadi kebutuhan yang signifikan dalam pengelolaan kualitas layanan yang diberikan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang dikelola. Hal tersebut tentunya didukung dengan pengelolaan aset informasi yang dimiliki termasuk pusat data (*data center).*

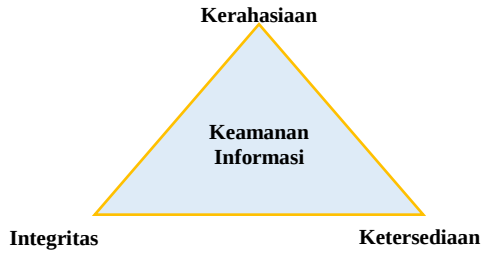
Pusat data dalam organisasi memiliki peranan yang sangat penting. Kegagalan pusat data biasanya memiliki dampak signifikan, karena hilangnya akses ke informasi dapat menimbulkan biaya yang sangat tinggi. Berbagai ancaman, termasuk gangguan teknis

Diterima: 23-05-2025 | Revisi: 20-06-2025 | Diterbitkan: 28-06-2025 | doi: 10.37034/infeb.v7i2.1160

dan kesalahan manusia, dapat menyebabkan kegagalan tersebut. Upaya yang dilakukan untuk mengurangi risiko tersebut antara lain dengan memenuhi standar dan melaksanakan praktik terbaik [4]. Selain itu, langkah proaktif juga perlu dilakukan untuk menilai dan menganalisis potensi ancaman yang dapat mengganggu integritas, kerahasiaan, dan ketersediaan data yang disimpan dan diproses dalam *pusat data*. Ancaman tersebut dapat menjadi risiko bagi organisasi yang perlu diukur untuk mencegah dampak yang mungkin terjadi.

Project Management Institute mendefinisikan risiko sebagai kejadian yang tidak pasti atau tidak terduga yang dapat memengaruhi tujuan proyek apabila terjadi [5][6]. Risiko dapat berasal dari satu atau lebih sumber dan dapat menimbulkan satu atau lebih dampak. Tingkat toleransi para pemangku kepentingan terhadap risiko bervariasi karena sejumlah faktor, seperti kemungkinan terjadinya, dampaknya terhadap fasilitas, persepsi, serta sikap dan toleransi individu terhadap risiko [6]. Risiko dipengaruhi oleh kejadian di masa lalu dan masa kini, serta strategi mitigasi yang diterapkan. Sehingga, memahami dan memantau kejadian masa lalu dan masa kini menjadi penting untuk memperoleh gambaran yang lebih baik tentang potensi risiko di masa depan [7].

Keamanan informasi adalah memastikan kerahasiaan, ketersediaan, dan integritas data. Ruang lingkup keamanan informasi tidak terbatas pada informasi digital, tetapi juga hal-hal lain seperti kertas dan pengetahuan manusia. Salah satu tujuan keamanan informasi umumnya adalah untuk mengurangi risiko dalam menjalankan bisnis, atau dengan kata lain, manajemen risiko [6]. Selanjutnya pilar adalah kerahasian ditampilkan pada Gambar 1.

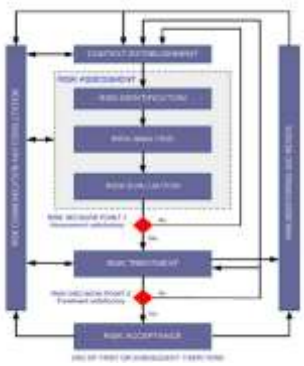


Gambar 1. Pilar adalah Kerahasiaan

Keamanan informasi memiliki tiga pilar seperti yang digambarkan pada Gambar 1. Ketiga pilar tersebut adalah kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) yang dikenal dengan istilah CIA [7]. Kerahasiaan memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Integritas menjamin data tetap utuh dan tidak dapat diubah atau dimodifikasi tanpa izin, serta memastikan keakuratan informasi. Ketersediaan memastikan bahwa data selalu dapat diakses ketika diperlukan. Ketiga aspek CIA ini harus diimplementasikan secara optimal dalam sebuah pusat data. Ketiga aspek CIA tersebut harus diterapkan dengan baik dalam sebuah pusat data.

Pusat data adalah fasilitas yang menyediakan berbagai sumber daya untuk memproses, menyimpan, dan mendistribusikan informasi digital. Fasilitas ini mencakup perangkat teknologi informasi (TI) beserta infrastruktur pendukungnya, seperti sistem kelistrikan, pendinginan, telekomunikasi, perlindungan kebakaran, keamanan, dan sistem otomatisasi [8]. Operasional pusat data didukung oleh berbagai fasilitas, termasuk sistem manajemen daya, pengaturan suhu udara, perlindungan kebakaran, serta sistem keamanan fisik. Dalam pengoperasiannya pusat data jutaan hingga miliaran data diproses dan ditransfer melalui pusat data, sehingga untuk mengelola informasi tersebut membutuhkan kapasitas komputasi dan penyimpanan yang besar. Proses pengolahan data ini harus dilakukan dengan baik dan optimal karena pusat data menjadi salah satu aset paling penting bagi sebuah organisasi.

ISO 27005 menyediakan panduan untuk manajemen risiko keamanan informasi dan dirancang untuk mendukung penerapan proses keamanan informasi dengan pendekatan berbasis manajemen risiko. Standar ini dapat diterapkan oleh berbagai jenis organisasi, termasuk perusahaan komersial, lembaga pemerintah, dan organisasi nirlaba, yang bertujuan mengelola risiko yang dapat mengancam keamanan informasi [9]. ISO 27005 merupakan bagian dari keluarga standar ISO 27000. Mengacu pada ISO 27001, organisasi dapat membentuk komite keamanan informasi untuk menyusun kebijakan terkait keamanan informasi. ISO 27005 secara khusus membahas manajemen risiko keamanan informasi, dengan pembaruan terakhir dirilis pada tahun 2022. Penilaian risiko sesuai dengan kerangka kerja ISO 27005 menyediakan panduan langkah demi langkah, mencakup penetapan konteks, penilaian risiko keamanan informasi, penanganan risiko, penerimaan risiko, komunikasi risiko, serta pemantauan dan evaluasi risiko keamanan informasi [10]. Ilustrasi dari alur kerja ISO 27005 dapat ditampilkan pada Gambar 2.



Gambar 2. Alur Kerja dari ISO 27005

Berbagai penelitian sebelumnya mengenai manajemen risiko telah banyak dilakukan dalam berbagai ruang lingkup, seperti sistem aplikasi, pusat data atau lingkup organisasi secara keseluruhan. Penelitian tersebut juga dilakukan dengan berbagai kerangka kerja. Adapun penelitian-penelitian sebelumnya dapat disajikan pada Tabel 1.

Tabel 1. Penelitian Terdahulu

Penelitian	Fokus Penelitian	Metode & Lingkup Penelitian	Kerangka Kerja
Putra & Mutijarsa	Merancang manajemen risiko keamanan informasi pada instansi pemerintah, Pusat Komando Kepolisian.	*Design Research Methodology* (DRM) pada Pusat Komando Kepolisian	ISO/IEC 27005:2018 dan NIST SP 800-30
Fikri dkk	Pengujian penerapan penilaian risiko dengan menggunakan kombinasi NIST SP 800-30 dan ISO 27005 pada perusahaan bisnis.	Semi-kuantitatif pada Sistem Aplikasi	NIST SP 800-30 dan ISO 27005
Fahrurozi dkk	Membuat perancangan manajemen keamanan informasi berdasarkan manajemen risiko di Pusat Pengolahan Data dan Teknologi Informasi, Pusdatin Kemhan.	*Design Research Methodology* (DRM) pada Pusat Pengolahan Data dan Teknologi Informasi.	ISO/IEC 27005:2018
Andry dkk	Melakukan analisis risiko pusat data pada perusahaan farmasi.	Metode Kualitatif pada pusat data	ISO 31000:2009
Putra dkk	Menyusun perencanaan manajemen risiko keamanan informasi pusat data.	Metode Kualitatif pada pusat data	ISO/IEC 27005:2018 dan NIST SP 800-30

Penilaian risiko keamanan informasi dapat dilakukan dengan berbagai metode dan kerangka kerja. Penggunaan ISO 31000 menekankan integrasi manajemen risiko dalam seluruh proses organisasi, termasuk tata kelola, strategi, dan pengambilan keputusan. Manajemen risiko dengan ISO 31000:2009 menyediakan prinsip dan proses manajemen risiko untuk meningkatkan kapabilitas perusahaan dalam menghadapi risiko untuk memanfaatkan peluang dan mengantisipasi risiko yang dapat memberikan dampak negatif bagi perusahaan [11]. Sedangkan manajemen risiko yang lebih spesifik terkait keamanan informasi dibahas pada ISO 27005 dan kerangka kerja NIST SP 800-30 digunakan untuk memberikan panduan penilaian risiko untuk organisasi dan sistem informasi pemerintah [12]. Penilaian risiko terkait pusat data pada instansi pemerintah akan lebih sesuai jika menggunakan ISO 27005 sebagai kerangka kerja dalam penilaian risiko yang dipadukan dengan NIST SP 800-30 yang memberikan panduan lebih teknis terkait penilaian risiko [13].

Dalam konteks penilaian risiko keamanan *pusat data*, berbagai kerangka kerja penilaian risiko telah berkembang sebagai standar yang dapat digunakan. ISO 27000: *Sistem Manajemen Keamanan Informasi* menawarkan panduan praktik terbaik untuk mengelola risiko informasi melalui berbagai kontrol [14]. ISO 31000: *Manajemen Risiko – Panduan* menjelaskan prinsip dan proses untuk mengelola risiko secara efektif, sedangkan NIST SP 800-30: *Kerangka Kerja Manajemen Risiko* menyediakan pedoman penerapan manajemen risiko pada organisasi federal [15]. Standar ISO 27005 direkomendasikan karena dapat digunakan diberbagai jenis organisasi, baik komersial, non-komersial, maupun lembaga pemerintah [16]. Standar ini menawarkan rekomendasi yang fleksibel sehingga dapat disesuaikan dengan berbagai studi kasus. Penerapan ISO 27005 juga berpotensi mendorong perbaikan berkelanjutan dalam proses pengambilan keputusan serta peningkatan kinerja organisasi [17].

Penilaian risiko keamanan informasi dengan menggunakan standar ISO 27005 diawali dengan mengidentifikasi aset-aset yang dimiliki untuk dilakukan analisis risiko. Penilaian risiko berdasarkan analisis aset belum dilakukan secara khusus untuk pusat data pada Instansi XYZ [18]. Oleh karena itu, penelitian ini bertujuan untuk menilai risiko keamanan informasi *pusat data* pada Instansi XYZ sehingga dapat memberikan masukan terkait peningkatan keamanan informasi di Instansi XYZ dengan menggunakan Standar ISO 27005 [19] dan NIST SP 800-30 [20]. Adapun pertanyaan penelitian yang diangkat dalam penelitian ini adalah bagaimana nilai risiko keamanan informasi pada Pusat Data Instansi XYZ?.

2. Metode Penelitian

Penelitian ini dilakukan dengan metode kualitatif yang dilakukan melalui studi dokumentasi dan wawancara dengan narasumber pegawai Instansi XYZ. Metode kualitatif dipilih untuk memfokuskan penelitian dalam mencapai tujuan penelitian yaitu bagaimana nilai risiko keamanan informasi Pusat Data Instansi XYZ. Penilaian dilakukan sesuai dengan kerangka kerja ISO 27005: 2018 dan NIST SP 800-30. Pada penelitian ini dilakukan pengumpulan data melalui berbagai sumber untuk mendapatkan data primer dan data sekunder.

Pengumpulan data diawali dengan pengumpulan data sekunder dari studi literatur terkait penilaian risiko keamanan informasi dari dokumen publik yang terdiri dari berita, *paper*, dan artikel ilmiah lainnya sebagai referensi dalam pelaksanaan penelitian. Pengumpulan data primer dilakukan dengan mengumpulkan dokumen internal dari Instansi XYZ yang terdiri dari data regulasi, laporan tahunan, dan dokumen aset yang dimiliki. Pengumpulan data juga dilakukan melalui wawancara kepada pegawai Instansi XYZ selaku pengelola pusat data yang telah bekerja lebih dari lima tahun. Penentuan narasumber dilakukan dengan *purposive sampling*.

Data yang telah berhasil dikumpulkan kemudian dilakukan pengolahan data untuk melakukan penilaian risiko keamanan informasi sesuai dengan kerangka kerja ISO 27005: 2018 dan dengan komposisi teknis penilaian risiko berdasarkan NIST SP 800-30. Dalam

hal pertimbangan menilai risiko keamanan informasi didasarkan pada pemilik informasi yang dijadikan sebagai narasumber. Langkah-langkah yang dilakukan dalam analisis data ditampilkan pada Gambar 3.

Gambar 3. Tahapan Analisis Data

Analisis data diawali dengan melakukan penetapan konteks risiko keamanan informasi yang terdiri dari inventarisasi informasi umum, ruang lingkup, kategori, kriteria, matriks analisis risiko dan level risiko. Selanjutnya dilakukan penilaian risiko yang terdiri dari 3 tahapan yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko. Pada identifikasi risiko dilakukan proses menggali informasi mengenai kejadian, penyebab, dan dampak risiko. Identifikasi risiko ini diawali dengan melakukan identifikasi aset-aset yang ada pada pusat data Intsansi XYZ. Analisis risiko dilakukan dengan cara menentukan sistem pengendalian, level kemungkinan, dan level dampak terjadinya risiko dari hasil identifikasi risiko yang telah dilakukan. Evaluasi risiko dilakukan untuk mengambil keputusan mengenai perlu tidaknya dilakukan upaya penanganan risiko lebih lanjut serta penentuan prioritas penanganannya.

Pada tahap akhir dilakukan validasi hasil penilaian untuk memvalidasi hasil penilaian risiko keamanan informasi pada pusat data yang dilakukan melalui wawancara dengan pegawai dari Instansi XYZ. Pada tahapan ini juga menjelaskan kepada narasumber hasil evaluasi risiko yang dapat dilakukan sebagai bahan pertimbangan dalam pengambilan keputusan dari penanganan risiko di Pusat Data Instansi XYZ.

3. Hasil dan Pembahasan

Pada tahap ini, analisis hasil penelitian pada Pusat Data Instansi XYZ berfokus pada langkah-langkah penilaian risiko keamanan informasi berdasarkan standar ISO/ 27005:2018 dan NIST SP 800-30. Penentuan konteks risiko mencangkup penentuan inventarisasi informasi umum, ruang lingkup, dan batasan untuk penilaian risiko keamanan informasi. Selain itu, penentuan konteks juga menentukan kriteria dampak, kriteria kemungkinan dan kriteria penerimaan risiko sebelum dilakukan proses penilaian risiko keamanan informasi di Pusat Data Instansi XYZ.

Penilaian risiko keamanan informasi dilakukan pada Instansi XYZ, dengan unit pemilik risiko adalah Pusat Teknologi Informasi Instansi XYZ. Ruang lingkup penerapan pelaksanaan penilaian risiko adalah pusat data yang ada pada Instansi XYZ. Kriteria evaluasi risiko harus dikembangkan untuk mengevaluasi risiko keamanan informasi dalam organisasi. Dalam konteks penelitian ini risiko kriteria evaluasi ditentukan berdasarkan kerahasiaan, integritas, dan ketersediaan operasional. Kriteria dampak berhubungan dengan tingkat kerusakan atau penurunan layanan organisasi yang disebabkan oleh insiden keamanan informasi. Berdasarkan hasil studi dokumentasi internal, kriteria dampak disajikan pada Tabel 2.

Tabel 1. Kriteria Dampak

Level Dampak	Keterangan		Nilai Dampak
	Penurunan Layanan Organisasi	Kerusakan	
Tidak signifikan	Operasional: <25% dari jam operasional layanan harian	Kerusakan sedikit atau tidak berpengaruh	1
Minor	Operasional: 25%-50% dari jam operasional layanan harian	Kerusakan minimal	2
Moderate	Operasional: 50%-75% dari jam operasional layanan harian	Kerusakan atau dampak besar	3
Signifikan	Operasional: 75%-100% dari jam operasional layanan harian	Kerusakan kritis atau dampak negatif jangka panjang	4
Sangat Signifikan	-	kerusakan yang sangat besar dan konsekuensi yang tidak dapat diperbaiki	5

Kriteria penerimaan risiko terkait dengan kebijakan dan tujuan para pemangku kepentingan berdasarkan selera risiko. Penentuan selera risiko didasarkan pada tingkat kemungkinan dan dampak. Tabel 3 menjelaskan matriks selera risiko di Instansi XYZ. Untuk risiko dengan nilai risiko diatas 9 maka risiko ersebut dilakukan mitigasi, namun jika berada dibawah nilai risiko 9 maka risiko dapat diterima. Untuk mempermudah menilai risiko dapat dilihat level risiko sesuai besarannya pada Tabel 4.

Tabel 2. Kriteria Penerimaan Risiko

		Level Dampak				
		1	2	3	4	5
Level Kemungkinan	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Tabel 3. Level Besaran Risiko

Level Risiko	Besaran Risiko	Warna
Sangat Tinggi (5)	20 - 25	Merah
Tinggi (4)	15 - 19	Oranye
Sedang (3)	9 - 14	Kuning
Rendah (2)	5 - 8	Hijau
Sangat Rendah (1)	1 - 4	Biru

Tabel 4. Kriteria Kemungkinan

Level Kemungkinan	Kriteria Kemungkinan		
	Non Low Tolerance Event Dalam 1 Periode		*low tolerance event*
	Persentase Kemungkinan	Jumlah Frekuensi	
Hampir tidak mungkin terjadi (1)	<= 20%	<= 3 kali	< 1 kejadian dalam lebih dari 5 tahun terakhir
Kemungkinan kecil terjadi (2)	21% - 40%	4 - 6 kali	1 kejadian dalam lebih dari 5 tahun terakhir
Kemungkinan terjadi dan tidak terjadi sama besar (3)	41% - 60%	7 - 9 kali	1 kejadian dalam 3 tahun terakhir
Kemungkinan besar terjadi (4)	61% - 80%	10 - 12 kali	1 kejadian dalam 2 tahun terakhir
Hampir pasti terjadi (5)	>= 81%	> 12 kali	Minimal 1 kejadian dalam 1 tahun terakhir

Identifikasi risiko dilakukan untuk menggali informasi mengenai kejadian, penyebab, dan dampak risiko. Identifikasi risiko diawali dengan melakukan identifikasi aset-aset yang ada pada pusat data Intsansi XYZ, dilanjutkan dengan identifikasi ancaman, identifikasi eksisting kontrol dan identifikasi kerentanan yang ada pada pusat data Instansi XYZ. Langkah pertama dalam penilaian risiko adalah mengidentifikasi aset yang dimiliki. Proses ini dimulai dengan membuat daftar aset yang masuk kedalam pusat data dan dianggap penting bagi keamanan informasi. Dalam penelitian ini, aset yang diidentifikasi mencapai 20 jenis yang dikelompokkan menjadi dua kategori yaitu aset utama dan aset pendukung. Aset utama merupakan aset yang secara langsung terkait dengan layanan instansi dan memiliki nilai kritis terhadap proses bisnis. Aset utama yang teridentifikasi ada tiga yaitu dari data proses bisnis Instansi XYZ, data kepegawaian dan termasuk di dalamnya pegawai Instansi XYZ.

Aset pendukung adalah aset yang mendukung aset utama dalam menjalankan fungsinya namun tidak secara langsung terkait dengan layanan proses bisnis. Aset pendukung yang teridentifikasi berjumlah 17 aset yang terdiri dari tiga kategori yaitu, infrastruktur server, jaringan, dan aplikasi. Aset yang menjadi bagian dari infrastruktur server adalah server aplikasi, server database, server host virtual, server virtual aplikasi kepegawaian, SAN storage, keyboard, video, moitor (KVM), rak server, dan rak server jaringan. Aset yang termasuk dalam kategori jaringan terdiri dari router, core switch, firewall, web application firewall (WAF), Intrusion Preventive System (IPS), kabel ethernet dan kabel *fiber oftic* (FO). Untuk aset yang masuk dalam kategori aplikasi adalah aplikasi layanan Instansi XYZ dan aplikasi kepegawaian. Keduapuluh aset tersebut diberikan kode A01 hingga A20 seperti yang disajikan pada Tabel 6.

Tabel 5. Daftar Identifikasi Aset

Kode	Jenis Aset	Nama Aset	Kategori
A01	Utama	Data proses bisnis Instansi XYZ	-
A02	Utama	Data Kepegawaian	-
A03	Utama	Pegawai	-
A04	Pendukung	Server Aplikasi	Infrastruktur
A05	Pendukung	Server Database	Infrastruktur
A06	Pendukung	Server Host Virtual	Infrastruktur
A07	Pendukung	SAN Storage	Infrastruktur
A08	Pendukung	Keyboard, Video, Monitor (KVM)	Infrastruktur
A09	Pendukung	Rak Server	Infrastruktur
A10	Pendukung	Rak Jaringan	Infrastruktur
A11	Pendukung	Server Virtual Aplikasi Kepegawaian	Infrastruktur
A12	Pendukung	Router	Jaringan
A13	Pendukung	Core Switch	Jaringan
A14	Pendukung	Firewall	Jaringan
A15	Pendukung	Web Application Firewall (WAF)	Jaringan
A16	Pendukung	Intrusion Preventive System (IPS)	Jaringan
A17	Pendukung	Kabel Ethernet	Jaringan
A18	Pendukung	Kabel Fiber Optic (FO)	Jaringan
A19	Pendukung	Aplikasi Layanan Instansi XYZ	Aplikasi
A20	Pendukung	Aplikasi Kepegawaian	Aplikasi

Identifikasi ancaman dilakukan untuk mengidentifikasi sumber ancaman dan kejadian yang mungkin terjadi. Sumber ancaman diklasifikasikan menjadi dua kategori utama, yaitu ancaman yang bersifat adversarial (bermotif jahat) dan non-adversarial (tidak disengaja). Identifikasi ancaman diperoleh dari observasi referensi ancaman dari ISO 27005: 2018 yang disesuaikan dengan riwayat ancaman yang timbul pada Instansi XYZ. Dari hasil Identifikasi ancaman diperoleh 27 ancaman, dengan kode T01 hingga T027. Ringkasan daftar ancaman dapat disajikan pada Tabel 7. Dari 27 ancaman tersebut, diklasifikasikan menjadi enam jenis ancaman. Enam ancaman dari kegagalan teknis, 3 ancaman dari kehilangan layanan penting, tujuh ancaman dari kerusakan fisik, empat ancaman dari perilaku manusia, tiga ancaman dari peristiwa alam, dan empat ancaman dari tindakan tidak sah.

Tabel 6. Identifikasi Ancaman

Kode	Ancaman	Jenis Ancaman
T01	Kegagalan peralatan atau perangkat keras	Kegagalan Teknis
T07	Hilangnya pasokan listrik	Kehilangan Layanan yang Penting
T10	Api	Kerusakan Fisik
T17	Hacker, Kriminal, Teroris, Spionase (Attacker)	Perilaku Manusia
T23	Rekayasa data	Tindakan yang Tidak Sah
T….	….....	……
T27	Keselamatan Jiwa	Peristiwa Alam

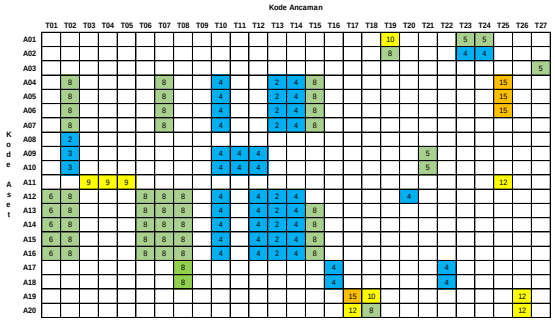
Potensi risiko dapat terjadi karena adanya kerentanan akibat tidak adanya kontrol terhadap risiko atau kontrol yang sudah ada namun kurang efektif/efisien dalam menangani ancaman yang terjadi. Berdasarkan ISO 27001 ada tiga belas kategori kontrol yang sudah teridentifikasi dimulai dari kategori kebijakan

keamanan informasi hingga kontrol kepatuhan kebijakan kemanan informasi.

Identifikasi kerentanan ditujukan untuk mengidentifikasi dan menilai kerentanan yang dipengaruhi oleh sumber aset dan jenis ancaman. Identifikasi dilakukan berdasarkan hasil observasi referensi ancaman dari ISO 27005 dan disesuaikan dengan kondisi eksisting Instansi dengan hasil 49 kerentanan yang teridentifikasi. Dari kerentanan yang ada akan dilakukan penilaian risiko oleh pihak pengelola pusat data, sehingga diperoleh nilai risiko terhadap aset pusat data.

Tahap analisis risiko merupakan inti dari penilaian risiko. Analisis risiko dilakukan dengan menentukan tingkat dampak yang ditimbulkan jika ancaman dari setiap aset berhasil dieksploitasi. Penentuan tingkat kecenderungan ini dinilai dari hasil wawancara dari narasumber pengelola Pusat Data Instansi XYZ. Nilai risiko diperoleh dari hasil perkalian dari penilaian terhadap level kemungkinan munculnya ancaman dengan penilaian level dampak terhadap proses bisnis di Instansi XYZ sesuai dengan kriteria yang telah ditentukan pada tahap penetapan konteks risiko.

Tabel 8. Matrik Risiko



Dari hasil analisis risiko terhadap 20 aset pusat data diperoleh 111 risiko yang terdiri dari 48 risiko pada level sangat rendah, 50 risiko pada level rendah, 9 risiko pada level sedang, dan 4 risiko pada level tinggi. Level risiko tersebut dapat dilihat pada matrik risiko pada Tabel 8. Risiko pada level tinggi berjumlah empat risiko yang berasal dari aset server aplikasi, server database, server host virtual, dan aplikasi. Risiko tersebut muncul dari ancaman T27 dan T17 yaitu serangan *malware* dan *hacker*. Sedangkan risiko pada level sedang yang berjumlah sembilan risiko muncul dari empat aset pusat data, yaitu data layanan instansi, server virtual aplikasi kepegawaian, aplikasi layanan instansi dan aplikasi kepegawaian. Risiko pada level sedang muncul dari ancaman kerusakan peralatan atau perangkat keras (T03), kejenuhan sistem informasi (T04), kerusakan perangkat lunak (T05), serangan hacker (T17), penyalahgunaan hak (T18), korupsi data (T19), serangan malware (T25), dan serangan DDoS (T26).

Evaluasi risko dilakukan dengan melihat selera risiko di Instansi XYZ. Sesuai dengan ISO 27005 terdapat empat pilihan dalam pengelolaan risiko yaitu, mitigasi risiko (*mitigate*), membagi risiko (*sharing*), menghindari risiko ((*avoide)*, dan menerima risiko (*accept*). Berdasarkan kriteria penerimaan risiko yang ada pada Instansi XYZ, diperoleh 13 risiko yang perlu dimitigasi, terdiri dari 4 risiko pada level tinggi dan 9 risiko pada level sedang. Sementara itu, 98 risiko lainnya dianggap dapat diterima. Tabel evaluasi prioritas risiko dapat disajikan pada Tabel 9.

Tabel 7. Prioritas Risiko

Prioritas	Skenario	Level Risiko	Level Risiko	Selera Risiko
1	A04, T25	15	Tinggi	Mitigasi
2	A05, T25	15	Tinggi	Mitigasi
3	A06, T25	15	Tinggi	Mitigasi
4	A19, T17	15	Tinggi	Mitigasi
5	A11, T25	12	Sedang	Mitigasi
6	A19, T26	12	Sedang	Mitigasi
7	A20, T17	12	Sedang	Mitigasi
8	A20, T26	12	Sedang	Mitigasi
9	A01, T19	10	Sedang	Mitigasi
10	A19, T18	10	Sedang	Mitigasi
11	A11, T03	9	Sedang	Mitigasi
12	A11, T04	9	Sedang	Mitigasi
13	A11, T05	9	Sedang	Mitigasi
14	A02, T19	8	Rendah	Diterima
15	A04, T02	8	Rendah	Diterima
16	A04, T07	8	Rendah	Diterima
17	A04, T15	8	Rendah	Diterima
18	A05, T02	8	Rendah	Diterima
.....	.....	.....	.....	.....
111	A16, T13	2	Sangat Rendah	Diterima

13 risiko yang perlu dimitigasi berasal dari tujuh aset pusat data, yaitu risiko level tinggi yang terdapat pada aset server aplikasi, server database, server host virtual, dan aplikasi. Risiko level sedang yang muncul dari aset data layanan instansi, server virtual aplikasi kepegawaian, aplikasi layanan instansi, dan aplikasi kepegawaian.

4. Kesimpulan

Berdasarkan hasil penilaian risiko di Pusat Data Instansi XYZ, teridentifikasi 111 risiko yang terbagi ke dalam empat kategori yaitu 48 risiko berada pada level sangat rendah, 50 risiko pada level rendah, 9 risiko pada level sedang, dan 4 risiko pada level tinggi. Risiko-risiko tersebut berasal dari 20 aset pusat data yang menghadapi 27 jenis ancaman dan 49 kerentanan yang telah teridentifikasi. Berdasarkan kriteria penerimaan risiko yang ada pada Instansi XYZ, terdapat 13 risiko yang perlu dimitigasi, terdiri dari 4 risiko pada level tinggi dan 9 risiko pada level sedang. Sementara itu, 98 risiko lainnya dianggap dapat diterima. Dari 13 risiko tersebut Instansi XYZ perlu melakukan tindakan mitigasi terhadap tujuh aset pusat data yang terdiri dari aset server aplikasi, server database, server host virtual, aplikasi layanan instansi, data layanan instansi, server virtual aplikasi kepegawaian, dan aplikasi kepegawaian. Tindakan mitigasi yang dilakukan dapat mengacu pada kontrol yang ada pada ISO 27002 terkait kendali keamanan informasi. Penelitian ini fokus pada penilaian risiko terhadap aset yang ada pada pusat data sehingga penelitian selanjutnya dapat melakukan kajian terkait kontrol yang dapat diimplementasikan terhadap risiko-risiko yang ada pada aset pusat data.

Daftar Rujukan

[1] Hero, A., Kar, S., Moura, J., Neil, J., Poor, H. V., Turcotte, M., & Xi, B. (2023). Statistics and Data Science for Cybersecurity. *Harvard Data Science Review*, *5*(1). DOI: https://doi.org/10.1162/99608f92.a42024d0 .

[2] Hariani, H., Darmatasia, D., & Saputra, W. (2020). Capability Maturity Model Integration (Cmmi) untuk Analisis Keamanan Informasi Menggunakan Domain Apo13 Cobit 5 pada Pustipad Instansi X. *Jurnal INSYPRO (Information System and Processing)*, *5*(2). DOI: https://doi.org/10.24252/insypro.v5i2.19751 .

[3] Levy, M. (2020). A Novel Framework for Data Center Risk Assessment. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2020 (pp. 0148–0154). *Institute of Electrical and Electronics Engineers Inc.* DOI: https://doi.org/10.1109/UEMCON51285.2020.9298072 .

[4] Rose, K. H. (2013). A Guide to the Project Management Body of Knowledge (PMBOK Guide) Fifth Edition. *Project Management Journal*, *44*(3), e1–e1. DOI: https://doi.org/10.1002/pmj.21345 .

[5] Hwang, B. G., Zhu, L., & Tan, J. S. H. (2017). Green Business Park Project Management: Barriers and Solutions for Sustainable Development. *Journal of Cleaner Production*, *153*, 209–219. DOI: https://doi.org/10.1016/j.jclepro.2017.03.210 .

[6] Putra, I. M. M., & Mutijarsa, K. (2021). Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005. In 3rd 2021 East Indonesia Conference on Computer and Information Technology, EIConCIT 2021 (pp. 14–19). *Institute of Electrical and Electronics Engineers Inc.* DOI: https://doi.org/10.1109/EIConCIT50028.2021.9431865 .

[7] Tipton, H. F., & Krause, M. (2008). Information Security Management Handbook. *Information Security Management Handbook, Sixth Edition* (Vol. 2, pp. 1–437). CRC Press. DOI: https://doi.org/10.1201/9781420067101 .

[8] Al Fikri, M., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique In Profit-Based Organization: Case Study Of ZZZ Information System Application In ABC Agency. *In Procedia Computer Science* (Vol. 161, pp. 1206–1215). Elsevier B.V. DOI: https://doi.org/10.1016/j.procs.2019.11.234 .

[9] Kim, Y., & Kim, B. (2021). The Effective Factors on Continuity of Corporate Information Security Management: Based On Toe Framework. *Information (Switzerland)*, *12*(11). DOI: https://doi.org/10.3390/info12110446 .

[10] Andry, J. F., Liliana, L., Tannady, H., & Arief, A. S. (2022). Data Centre Risk Analysis Using ISO 31000:2009 Framework. In Journal of Physics: *Conference Series* (Vol. 2394). Institute of Physics. DOI: https://doi.org/10.1088/1742-6596/2394/1/012032 .

[11] Fachrezi, M. I. (2021). Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000:2018 Diskominfo Kota Salatiga. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *8*(2), 764–773. DOI: https://doi.org/10.35957/jatisi.v8i2.789 .

[12] Munodawafa, F., & Awad, A. I. (2018). Security Risk Assessment Within Hybrid Data Centers: A Case Study of Delay Sensitive Applications. *Journal of Information Security and Applications*, *43*, 61–72. DOI: https://doi.org/10.1016/j.jisa.2018.10.008 .

[13] Turang, D. A. O., & Turang, M. C. (2020). Analisis Audit Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework Cobit 5 pada Instansi X. *Klik - Kumpulan Jurnal Ilmu Komputer*, *7*(2), 130. DOI: https://doi.org/10.20527/klik.v7i2.316 .

[14] Benyamin, J., & Almubaroq, H. Z. (2021). Penilaian Sistem Keamanan Informasi Data Center pada Instansi Yaza untuk Mencegah Ancaman Siber dalam Meningkatkan Pertahanan Negara. Infotronik : *Jurnal Teknologi Informasi dan Elektronika*, *6*(2), 77. DOI: https://doi.org/10.32897/infotronik.2021.6.2.1123 .

[15] Agustina, E. R., & Achmad, F. (2019). Perancangan Spesifikasi Keamanan Kontrol Akses pada Aplikasi Layanan Informasi di Lingkungan Instansi Pemerintah. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *6*(2), 195–200. DOI: https://doi.org/10.25126/jtiik.2019621304 .

[16] Hariani, H., Darmatasia, D., & Saputra, W. (2020). Capability Maturity Model Integration (CMMI) untuk Analisis Keamanan Informasi Menggunakan Domain Apo13 Cobit 5 pada Pustipad Instansi X. *Jurnal INSYPRO (Information System and Processing)*, *5*(2). DOI: https://doi.org/10.24252/insypro.v5i2.19751 .

[17] Wijatmoko, T. E. (2020). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Kantor Wilayah Kementerian Hukum dan Ham Diy. *Cyber Security dan Forensik Digital*, *3*(1), 1–6. DOI: https://doi.org/10.14421/csecurity.2020.3.1.1951 .

[18] Putri, T. S., Mutiah, N. M., & Prawira, D. P. (2022). Analisis Manajemen Risiko Keamanan Informasi Menggunakan Nist Cybersecurity Framework dan ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat). *Coding Jurnal Komputer Dan Aplikasi*, *10*(02), 237. DOI: https://doi.org/10.26418/coding.v10i02.54972 .

[19] Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. *Creative Information Technology Journal*, *4*(4), 264. DOI: https://doi.org/10.24076/citec.2017v4i4.119 .

[20] Xiuguo, W. (2018). A Security-Aware Data Replica Placement Strategy Based On Fuzzy Evaluation In The Cloud. *Journal of Intelligent and Fuzzy Systems*, *35*(1), 243–255. DOI: https://doi.org/10.3233/JIFS-169584 .