Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 4 Oktober 2024 Hal. 649-656
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

Manajemen Risiko pada Sistem Informasi Akademik Universitas XYZ Menggunakan ISO 27005:2018

Zefanya Valencia Leasa[a], Grandys Frieska Prassida[b]
[a]Sistem Informasi, Universitas Internasional Semen Indonesia, zefanya.leasa20@student.uisi.ac.id
[b]Sistem Informasi, Universitas Internasional Semen Indonesia, grandys.prassida@uisi.ac.id

Submitted: 25-06-2024, Reviewed: 09-07-2024, Accepted 09-09-2024
https://doi.org/10.47233/jteksis.v6i4.1459

Abstract
XYZ University is very likely to face security risks in the implementation of the Academic Information System (SIAKAD), which includes various threats such as cyber attacks, data leaks, and unauthorized use of data. Therefore, this study aims to identify information security risks with an approach that follows the ISO 27005:2018 standard. The research method used involves several important stages in ISO 27005:2018, starting from determining a clear scope and context as a basis for identifying, analyzing, and evaluating and determining appropriate actions against information security risks. The results of this study indicate that there are 4 data-related risks, 3 software-related risks, 6 hardware-related risks, and 5 risks in the people category, which have been identified. From the results of the analysis, there is 1 risk with an extreme level and 10 high-level risks. After evaluating the implementation of existing controls, there are 6 risks that exceed the risk acceptance level so that special actions are needed to manage these risks. Ultimately, this study contributes theoretically to the application of ISO 27005:2018 to analyze information security risks within the University. In addition, this study provides practical benefits for University management to be able to determine the right strategies and actions in managing information security risks.
Keywords: *Risk, Information Technology, Information Security, Academic Information Systems, ISO 27005:2018*

Abstrak
Universitas XYZ sangat mungkin menghadapi risiko keamanan dalam implementasi Sistem Informasi Akademik (SIAKAD), yang mencakup berbagai ancaman seperti serangan siber, kebocoran data, dan penggunaan data secara tidak sah. Oleh karena itu, penelitian ini bertujuan untuk mengidentifikasi risiko keamanan informasi dengan pendekatan yang mengikuti standar ISO 27005:2018. Metode penelitian yang digunakan melibatkan beberapa tahapan penting dalam ISO 27005:2018, dimulai dari penetapan ruang lingkup dan konteks yang jelas sebagai dasar untuk mengidentifikasi, menganalisis, dan mengavaluasi serta menentukan tindakan yang tepat terhadap risiko keamanan informasi. Hasil dari penelitian ini menunjukkan bahwa terdapat ada 4 risiko terkait data, 3 risiko terkait *software*, 6 risiko terkait *hardware*, dan 5 risiko dalam kategori *people*, yang telah terindentifikasi. Dari hasil analisis terdapat 1 risiko dengan level ekstrim dan 10 risiko level tinggi. Setelah dilakukan evaluasi penarapan kontrol eksisting, terdapat 6 risiko yang melebihi level penerimaan risiko sehingga perlu dilakukan tindakan khusus untuk mengelola risiko-risiko tersebut. Pada akhirnya, penelitian ini memberikan kontribusi secara teori dalam penerapan ISO 27005:2018 untuk menganalisis risiko keamanan informasi pada lingkup Universitas. Selain itu, penelitian ini memberikan manfaat praktis bagi manajemen Universitas untuk dapat mementukan strategi dan tindakan yang tepat dalam mengelola risiko keamanan informasi.
Keywords: Risiko, Teknologi Informasi, Keamanan Informasi, Sistem Informasi Akademik, ISO 27005:2018

PENDAHULUAN

Proses identifikasi risiko untuk Sistem Informasi Akademik (SIAKAD) memerlukan analisis yang komprehensif mengenai potensi bahaya yang dapat membahayakan integritas, kerahasiaan, dan aksesibilitas data akademik. Risiko dapat berasal dari berbagai sumber, termasuk faktor internal di dalam sistem dan faktor eksternal yang dapat mempengaruhi kinerja dan keamanan SIAKAD [1]. Ketika melakukan penilaian risiko pada Sistem Informasi Akademik (SIAKAD), penting untuk mengevaluasi dampak potensial terhadap kelangsungan operasional, kelangsungan proses akademik, dan reputasi Universitas XYZ. Selain itu, penilaian juga mencakup evaluasi terhadap kemungkinan terjadinya risiko, seperti kerentanan sistem terhadap serangan atau tingkat kesalahan manusia [2].

Evaluasi dampak risiko tidak hanya mencakup factor teknis, tetapi juga mempertimbangkan dampak pada keseluruhan operasi, proses akademik yang lancar, dan reputasi institusi. Dampak yang ditimbulkan dapat mencakup berbagai konsekuensi, termasuk tidak tersedianya layanan, potensi kerugian finansial, dan dampak yang merugikan terhadap reputasi Universitas XYZ. Kemungkinan risiko, seperti kerentanan sistem terhadap serangan siber atau tingkat kesalahan manusia, dinilai untuk

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 4 Oktober 2024 Hal. 649-656
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

menentukan probabilitas kemunculannya. Analisis ini membantu dalam menilai tingkat kesegeraan dan pentingnya manajemen risiko [3].

Dalam konteks khusus ini, Universitas XYZ menggunakan sistem yang mencakup beragam fungsi untuk membantu proses perkuliahan. Salah satu fungsi tersebut adalah SIAKAD, yang digunakan mahasiswa untuk menyederhanakan berbagai proses termasuk manajemen jadwal, penilaian mahasiswa, layanan akademik, dan prosedur penting lainnya. Selain itu, tidak adanya keamanan informasi dapat menimbulkan risiko seperti kebocoran data atau penggunaan data atau informasi yang tidak sah [4]. Menerapkan strategi manajemen risiko berdasarkan ISO 27005: 2018 merupakan langkah strategis yang dapat memberikan banyak keuntungan bagi Universitas XYZ, khususnya dalam konteks Sistem Informasi Akademik (SIAKAD) [5], [6]. Pendekatan ini bertujuan untuk membantu Universitas XYZ dalam memahami, mengendalikan, dan meminimalkan risiko keamanan informasi yang terkait dengan SIAKAD [7], [8].

Memanfaatkan kontrol ISO 27001 untuk mengelola sistem SIAKAD merupakan langkah penting untuk menjamin keamanan informasi yang efisien dalam lingkungan pendidikan. Dengan menggunakan standar internasional, Universitas XYZ dapat secara efektif mengidentifikasi, menilai, dan mengendalikan risiko keamanan informasi yang terkait dengan sistem SIAKAD mereka [9]. Selain itu, pendekatan manajemen berbasis risiko ISO 27001 memberdayakan organisasi untuk secara proaktif mengenali ancaman keamanan yang muncul dan mengambil tindakan yang tepat untuk mengatasinya [10]. Organisasi dapat meningkatkan kepercayaan diri mereka dalam mengelola data mahasiswa dan staf serta menjaga kelancaran proses akademik dengan melakukan audit dan penilaian independen secara teratur untuk memastikan penerapan kontrol keamanan informasi yang efektif dalam sistem SIAKAD mereka [11].

Penelitian sebelumnya yang dilakukan oleh I Putu Setyo Syahindra, dkk. pada tahun 2022 telah mengeksplorasi topik evaluasi risiko keamanan informasi di Diskominfo Provinsi XYZ. Penelitian tersebut berfokus pada penilaian tingkat kesiapan keamanan informasi instansi dan pengembangan strategi untuk meningkatkan manajemen keamanan informasi demi peningkatan kualitas layanan kepada para pemangku kepentingan. Studi ini menggunakan Indeks KAMI dan ISO:2011 sebagai kerangka kerja [12]. Jonny Jonny, Dkk melakukan penelitian berjudul "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005". Penelitian ini berfokus pada evaluasi potensi ancaman dan risiko yang terkait dengan ISO 27005 [13]. Penelitian yang dilakukan oleh Syasya Sahira,Dkk dengan judul Analisis Manajemen Risiko Pada Aplikasi E-office Yang Dikelola Oleh Pt Telkom Indonesia Menggunakan Standar Iso/iec 27005:2018 yang membahas tentang analisis manajemen risiko dilakukan untuk melindungi aset informasi yang terdapat disebuah aplikasi dari berbagai ancaman untuk minimalisir kebocoran data, pengunaan akses user, dan kesalahan pengembangan aplikasi selanjutnya [14]. Penelitian yang dilakukan oleh Ridho Fahlepi,Dkk dengan judul Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000 yang membahas tentang cara mendapatkan nilai RPN (Risk Priority Number) guna memberikan rekomendasi perlakuan risiko pada Sistem Informasi Akademik (SIAKAD) [15]. Penelitian yang dilakukan Abinel Santiago Cerqueira Junior and Carlos Hodio Arima dengan judul Cyber risk management and iso 27005 applied in organizations: a systematic literature review yang membahas tentang mengidentifikasi motivasi dan tujuan penerapan standar ISO 27005 dalam organisasi pada sistem produktif.Untuk pengembangan penelitian, dilakukan tinjauan literatur sistematis dengan adopsi protokol berdasarkan PRISMA-penerapan standar

ISO 27005 dalam organisasi pada sistem produktif.Untuk pengembangan penelitian, dilakukan tinjauan literatur sistematis dengan adopsi protokol berdasarkan PRISMA-P Hasilnya menunjukkan bahwa organisasi berusaha untuk mengadopsi ISO 27005 untuk memotivasi fungsional dan kelembagaan yang bertujuan untuk meningkatkan proses yang berkaitan dengan manajemen keamanan informasi, manajemen risiko, penilaian risiko, meningkatkan manajemen keamanan informasi dan memenuhi undang-undang, peraturan dan pemangku kepentingan [16].

METODE PENELITIAN

Penelitian ini menggunakan alur metode penelitian yang berurutan, dimulai dengan pemahaman yang komprehensif tentang Iso 27005: 2018. Selanjutnya, fokus akan bergeser ke arah identifikasi potensi risiko, dengan penekanan khusus pada identifikasi risiko yang mungkin timbul. Selanjutnya, risiko-risiko tersebut dievaluasi untuk menentukan tingkat dampak dan probabilitas terjadinya. Selanjutnya, risiko-risiko tersebut dinilai berdasarkan perspektif persepsi risiko, dengan mempertimbangkan bagaimana risiko-risiko tersebut dipahami oleh para pemangku kepentingan. Setelah evaluasi ini selesai, strategi manajemen risiko dirumuskan untuk memitigasi atau mengendalikan risiko yang telah diidentifikasi. Tahap selanjutnya adalah pelaksanaan dan

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 4 Oktober 2024 Hal. 649-656
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

pengawasan rencana strategis, di mana tindakan untuk memitigasi risiko diterapkan dan dipantau secara terus menerus. Hasil dari pengukuran dinilai dan dibahas dalam tahap hasil dan diskusi. Pada akhirnya, hasil evaluasi digunakan untuk menghasilkan kesimpulan dan rekomendasi, dengan tujuan untuk meningkatkan manajemen risiko di masa depan.

Gambar 1. Tahapan penelitian

2.1 Alur ISO 27005:2018

Manajemen risiko adalah prosedur sistematis yang melibatkan identifikasi, analisis, dan evaluasi risiko, diikuti dengan penerapan langkah-langkah untuk mengurangi dampak risiko pada proses. Proses manajemen risiko keamanan informasi yang dilakukan dalam penelitian ini menggunakan proses manajemen risiko yang diuraikan dalam ISO 27005. Teks selanjutnya memberikan penjelasan yang komprehensif tentang setiap fase yang terlibat dalam manajemen risiko keamanan informasi, seperti yang diuraikan oleh ISO 27005.

1. *Context Establishment*

Pembuatan konteks manajemen risiko keamanan informasi mencakup kriteria penilaian risiko, lingkup dan batasan, serta struktur organisasi manajemen risiko

2. *Risk Identification*

Proses mengidentifikasi, menggambarkan, dan memahami potensi risiko yang dapat mempengaruhi sebuah proyek, perusahaan, atau aktivitas lainnya. Tujuannya adalah untuk mengidentifikasi kemungkinan risiko yang mungkin terjadi agar dapat mengambil langkah-langkah pencegahan atau mitigasi yang tepat.

3. *Risk Analysis*

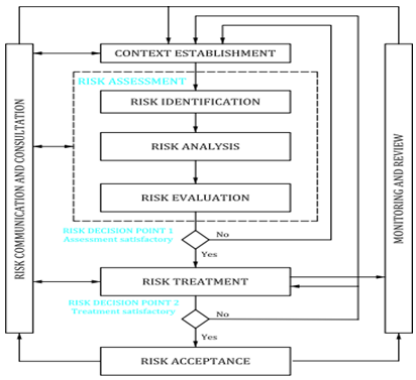
Proses untuk memahami dan mengevaluasi dampak potensial dari risiko yang telah diidentifikasi pada suatu proyek, kegiatan bisnis, atau organisasi. Tujuannya adalah untuk mengukur tingkat risiko yang terlibat dan membantu dalam pengambilan keputusan terkait strategi mitigasi atau penanganan risiko.

4. *Risk Evaluation*

Tahap penting dalam manajemen risiko di mana risiko-risiko yang telah diidentifikasi dan dianalisis akan dinilai lebih lanjut untuk menentukan tingkat keberhasilan proyek, aktivitas bisnis, atau tujuan lainnya dalam menghadapi risiko-risiko tersebut.

5. *Risk Treatment*

Langkah dalam manajemen risiko yang fokus pada pengembangan strategi untuk mengelola risiko-risiko yang sudah diidentifikasi dan dinilai dalam tahap sebelumnya.



Gambar 2. Alur ISO 27005:2018

2.2 Kontrol ISO 27001

ISO 27005 memberikan panduan tentang bagaimana mengelola risiko keamanan informasi secara holistik. Prosesnya dimulai dengan mengidentifikasi risiko-risiko yang mungkin terjadi terhadap keamanan informasi. Ini mencakup penilaian terhadap aset informasi yang penting, potensi ancaman, serta kerentanan yang ada dalam sistem informasi. Setelah itu, risiko-risiko tersebut dievaluasi berdasarkan dampak yang mungkin terjadi dan probabilitas terjadinya.

Kemudian, ISO 27001 hadir sebagai kerangka kerja untuk merancang, mengimplementasikan, dan memantau sistem manajemen keamanan informasi. Salah satu langkah penting dalam ISO 27001 adalah penentuan control keamanan yang tepat dengan risiko yang telah diidentifikasi. Ini termasuk kontrol fisik, teknis, dan kebijakan yang dirancang untuk mengurangi risiko, melindungi aset informasi, dan memastikan kelangsungan bisnis.

HASIL DAN PEMBAHASAN

3.1 Konteks, Ruang Lingkup dan Kriteria

1. Konteks

Sistem akademik adalah struktur yang mengatur dan mengelola semua aspek pendidikan di sebuah institusi pendidikan tinggi, seperti perguruan tinggi atau universitas. Ini mencakup serangkaian kegiatan, prosedur, dan kebijakan yang

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 4 Oktober 2024 Hal. 649-656
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

didesain untuk mendukung proses pembelajaran dan pengembangan mahasiswa.

Fungsi dari sistem akademik kampus sangatlah penting. Salah satunya adalah menyediakan landasan untuk menyusun kurikulum, yang mencakup berbagai mata pelajaran dan program studi yang ditawarkan. Tujuan dari sistem akademik kampus adalah menciptakan lingkungan pendidikan yang efektif dan mendukung perkembangan holistik mahasiswa.

2. Ruang Lingkup

Sistem akademik kampus mencakup berbagai elemen yang saling terkait, termasuk data/informasi,perangkat lunak (*software*), orang (*people*), dan perangkat keras (*hardware*). Perangkat lunak dalam sistem akademik kampus mencakup berbagai aplikasi yang digunakan untuk mengelola informasi, proses akademik, dan administrasi. Orang-orang yang terlibat dalam sistem akademik kampus meliputi mahasiswa, dosen, staf akademik, dan petugas administrasi. Mahasiswa menggunakan sistem untuk mengakses materi kuliah, mengikuti ujian, mengelola jadwal kuliah, dan berinteraksi dengan dosen serta sesama mahasiswa. Dosen dan staf akademik menggunakan sistem untuk mengelola materi kuliah, memberikan penilaian, berkomunikasi dengan mahasiswa, dan mengelola administrasi akademik. Sementara itu, pertugas administrasi bertanggung jawab atas manajemen data, pendaftaran mahasiswa, administrasi keuangan, dan layanan pelanggan terkait sistem akademik.

3. Kriteria

Tabel berikut menyajikan kriteria resiko yang relevan dengan penggunaan sistem informasi akademik (SIAKAD) di Universitas XYZ. Kriteria tersebut mencakup potensi kerugian keuangan, kendala dan keamanan sistem, serta aspek privasi yang perlu dipertimbangkan untuk menjaga integritas dan efektivitas SIAKAD tersebut. Dengan memahami dan mengukur resiko-resiko ini, universitas dapat mengambil langkah-langkah proaktif dalam pengelolaan dan pemantauan keamanan sistem mereka.

Tabel 1. Kriteria

Level	Kriteria	Kerugian Keuangan	Keandalan & Keamanan Sistem	Privasi
1	Langka	<0,5% Biaya Operasional	Aplikasi dan infrastruktur kritis mengalami downtime <5 menit	Kebocoran terbatas pada individu tertentu
2	Jarang Terjadi	<0,5% Biaya Operasional <1%	5 Menit < aplikasi kritis dan infratruktur mengalami downtime < 30 menit	Kebocoran terbatas pada individu tertentu
3	Memungkinkan	1% ≤ Biaya Operasional < 1,5%	30 Menit < aplikasi kritis dan infratuktur mengalami downtime < 1 jam	Terjadi kebocoran kurang dari 1% data privasi
4	Kemungkinan Besar	1,5% Biaya Operasional < 2%	1 Jam aplikasi kritis dan infratuktur mengalami downtime <4 jam	Ada kebocoran antara 2%-5% data privasi
5	Sangat Mungkin	Biaya Operasional > 2%	Aplikasi dan infrastruktur kritikal mengalami downtime > 4jam	Terjadi kebocoran lebih dari 5 % data privasi

A. *Risk Impact*

Berikut adalah gambar yang menggambarkan tingkat kemungkinan risiko yang terkait dengan penggunaan sistem informasi akademik (SIAKAD) di Universitas XYZ. Gambar ini mencakup level kemungkinan, penilaian kualitatif, dan penyesuaian berdasarkan sejarah risiko yang terjadi. Dengan memperhatikan informasi ini, universitas dapat mengidentifikasi dan mengelola risiko dengan lebih efektif, memastikan bahwa SIAKAD beroperasi secara aman dan efisien.

Tabel 2. Risk Impact

Level	Kualitatif	Penyesuaian Historis
1.	Langka	Kurang dari sekali dalam setahun
2.	Jarang Terjadi	1 Kali dalam 8 -10 bulan
3.	Memungkinkan	1 Kali dalam 5 - 8 bulan
4.	Kemungkinan Besar	1 Kali dalam 3 – 5 bulan
5.	Sangat mungkin	1 Kali dalam 1 -3 bulan

B. *Acceptance Risk*

Berikut ini adalah gambar *acceptance risk* yang menunjukkan tingkat penerimaan risiko terkait dengan penggunaan sistem informasi akademik (SIAKAD) di Universitas XYZ. Tabel ini menggunakan kombinasi tingkat kemungkinan dan konsekuensi risiko untuk menentukan apakah risiko dapat diterima atau tidak, dengan nilai risiko yang dapat diterima ketika tidak melebihi 6.

Tabel 3. Acceptance Risk

		Konsekuensi				
		1 Tidak Signifikan	2 Kecil	3 Sedang	4 Besar	5 Ekstrim
Kemungkinan	5 Sangat Mungkin	Sedang 5	Tinggi 10	Ekstrim 15	Ekstrim 20	Ekstrim 25
	4 Kemungkinan Besar	Sedang 4	Tinggi 8	Tinggi 12	Ekstrim 16	Ekstrim 20
	3 Memungkinkan	Rendah 3	Sedang 6	Tinggi 9	Tinggi 12	Ekstrim 15

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 4 Oktober 2024 Hal. 649-656
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

2 Jarang Terjadi	Rendah 2	Sedang 4	Sedang 6	Tinggi 8	Tinggi 10
1 Langka	Rendah 1	Rendah 2	Rendah 3	Sedang 4	Sedang 5

4. *Risk Identification*

Dengan mengenali ID risiko, jenis risiko, serta mengukur kemungkinan dan dampaknya, Universitas XYZ dapat memperkuat penggunaan sistem informasi akademik (SIAKAD) mereka. Melalui proses observasi dan penggalian pengalaman, hasilnya mengungkapkan beragam potensi risiko yang dapat memengaruhi efektivitas SIAKAD tersebut. Langkah-langkah ini memberikan landasan yang kokoh bagi universitas untuk mengelola dan meminimalkan risiko yang mungkin timbul.

Tabel 4. *Risk identification*

Risiko	Penyebab Risiko	Dampak Risiko Tinggi
Kebocoran data	Mahasiswa memberikan data kepada orang lain	Privasi, Keandalan Sistem, dan Keamanan
Kehilangan data	Terjadinya serangan malware	Privasi, Keandalan Sistem, dan Keamanan
Ketidakakuratan jadwal	Kesalahan input data sehingga bertabrakan dengan jadwal kelas lain	Keandalan Sistem dan Keamanan
Tidak adanya pembaruan data informasi	Staf akademik tidak melakukan update jika ada perubahan data	Keandalan Sistem dan Keamanan
Serangan siber	Kurangnya protokol keamanan	Keandalan Sistem, Keamanan, dan Privasi
Website tidak bisa diakses	Server yang mendukung website memiliki batasan dalam kapasitas	Keandalan Sistem dan Keamanan
Tidak responsif	Penggunaan ruang/RAM yang tinggi	Keandalan Sistem dan Keamanan
Kerusakan end user device	Kehilangan data yang sudah tersimpan	Privasi
Kerusakan end user device	Penggunaan end user secara berlebihan (overutilization)	Privasi
Kerusakan server	Terjadinya bencana alam	Keandalan Sistem dan Keamanan Kerugian Keuangan
Kerusakan server Server down	Terjadinya gangguan listrik	Keandalan Sistem dan Keamanan Kerugian Keuangan
Kegagalan perangkat keras	Downtime yang mengakibatkan kerusakan pada perangkat keras jaringan	Keandalan Sistem dan Keamanan
Gangguan kabel	Kabel yang rusak dan connector yang longgar dapat menyebabkan penurunan kinerja jaringan	Keandalan Sistem dan Keamanan
Developer kurang mampu menangani system crash	Ketergantungan terhadap satu developer	Keandalan Sistem dan Keamanan Kerugian Keuangan
Developer kurang mampu mengembangkan atau meningkatkan versi sistem	Pembuatan dokumentasi sistem yang tidak lengkap oleh developer sebelumnya	Keandalan Sistem dan Keamanan Kerugian Keuangan
Dosen memberikan data penting kepada pihak yang tidak berwenang	Ketidakpatuhan dosen terhadap kebijakan keamanan data dan sistem (masih share screen saat membuka tampilan SIAKAD dosen)	Privasi
Dosen melakukan kesalahan penggunaan sistem	Dosen yang belum terbiasa atau paham dengan cara keja sistem	Keandalan Sistem dan Keamanan Kerugian Keuangan
Mahasiswa salah menginputkan data	Mahasiswa yang tidak teliti membaca instruksi atau tidak teliti sebelum menginputkan data	Keandalan Sistem dan Keamanan Kerugian Keuangan

5. *Risk Analysis*

Tabel ini memperlihatkan analisis risiko inheren berdasarkan kemungkinan, dampak, nilai risiko, dan level risiko yang terkait dengan penggunaan SIAKAD. Selain itu, kontrol eksisting yang sudah diterapkan juga tercantum untuk menunjukkan langkah-langkah mitigasi yang sudah ada atau yang masih perlu ditingkatkan. Dengan informasi ini, Universitas XYZ dapat terus meningkatkan strategi pengelolaan risiko [17].

Tabel 5. *Risk analysis*

Data	ID Risk	Penyebab Risiko	Dampak Risiko Tertinggi	Risiko Inheren			
				K	D	Nilai Risi-ko	Level Risiko
Data	RD1	Mahasiswa memberikan data kepada orang lain	Privasi, Keandalan Sistem, dan Keamanan	2	5	10	Tinggi
	RD2	Terjadinya serangan malware	Privasi, Keandalan Sistem, dan Keamanan	1	5	5	Sedang
	RD3	Kesalahan input data sehingga bertabrakan dengan jadwal kelas lain	Keandalan Sistem, dan Keamanan	3	1	3	Rendah

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 4 Oktober 2024 Hal. 649-656
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

Data	ID Risk	Penyebab Risiko	Dampak Risiko Tertinggi	Risiko Inheren			
				K	D	Nilai Risi-ko	Level Risiko
	RD4	Staf Akademik tidak melakukan update jika ada perubahan data	Keandalan Sistem, dan Keamanan	3	2	6	Rendah
Soft-ware	RS1	Kurangnya protokol keamanan	Keandalan Sistem, Keamanan, dan Privasi	2	4	8	Tinggi
	RS2	Server yang mendukung website memiliki batasan dalam kapasitas	Keandalan Sistem, dan Keamanan	3	3	9	Tinggi
	RS3	Penggunaan browser yang tidak didukung atau versi yang sudah kedaluwarsa.	Keandalan Sistem, Keamanan, dan Privasi	2	4	8	Tinggi
Hard-ware	RH1	Kehilangan data yang sudah tersimpan	Privasi	2	5	10	Tinggi
	RH2	Penggunaan end user secara berlebihan (overutilization)	Privasi	2	5	10	Tinggi
	RH3	Tejadinya gangguan listrik	Keandalan Sistem dan Keamanan Kerugian Keuangan	2	4	8	Sedang
	RH4	Kerusakan pada hardware server	Keandalan Sistem, dan Keamanan	1	4	4	Tinggi
	RH5	Terjadinya serangan malware	Keandalan Sistem, dan Keamanan	3	4	12	Tinggi
	RH6	Kerusakan fisik pada perangkat keras jaringan	Keandalan Sistem, dan Keamanan	2	4	8	Sedang
People	RP1	Ketergantungan terhadap satu developer	Keandalan Sistem dan Keamanan Kerugian Keuangan	2	3	6	Tinggi
	RP2	Kurangnya fokus selama menginputkan data	Kerugian Keuangan	2	4	8	Tinggi
	RP3	Mahasiswa yang tidak teliti membaca instruksi atau tidak teliti sebelum menginputkan data	Keandalan Sistem dan Keamanan Kerugian Keuangan	2	4	8	Sedang
	RP4	Kurangnya kesadaran mahasiswa terhadap pentingnya kerahasiaan kunci akses akun SIAKAD nya	Privasi	3	2	6	Sedang
	RP5	Tidak adanya alur prosedur penyebaran informasi yang jelas ketika kampus merilis dokumen atau pedoman baru sehingga staff lupa update di SIAKAD	Keandalan Sistem, dan Keamanan	3	5	15	Ekstrim

6. *Risk Evaluation*

Berikut adalah tabel evaluasi risiko yang menggambarkan langkah-langkah dalam manajemen risiko terkait penggunaan sistem informasi akademik (SIAKAD) di Universitas XYZ. Kontrol yang telah ditetapkan disertakan dalam tabel untuk setiap risiko, mengenai pemilihan tindakan preventif/protektif juga disertakan, yang kemudian akan didokumentasikan dan dikomunikasikan secara internal. Hal ini memastikan bahwa langkah-langkah mitigasi risiko tidak hanya diterapkan secara efektif tetapi juga dipahami dan diikuti dengan konsisten oleh semua pemangku kepentingan terkait SIAKAD di universitas XYZ [18].

Tabel 6. *Risk evaluation*

ID Risk	Risiko	Kontrol Eksisting	Preventif/ Protektif	Risiko Residual			
				K	D	Nilai Risiko	Level Risiko
RD1	Kebocoran data	Pengecekan kebocoran data	Preventif	1	5	5	Sedang
RD2	Kehilangan data	Pencadangan informasi	Preventif	1	2	2	Rendah
RD3	Ketidakaku-ratan jadwal	Hak akses	Preventif	2	1	2	Rendah
RD4	Tidak adanya pembaruan data informasi	Kegiatan pemantauan	Preventif	2	2	4	Sedang
RS1	Serangan siber	Insiden keamanan informasi Perencanaan dan persiapan manajemen	Preventif	1	4	4	Sedang
RS2	Website tidak bisa diakses	Hak akses	Preventif	1	3	3	Rendah
RS3	Kehilangan integritas data	Kegiatan pemantauan	Tidak keduanya	2	4	8	Tinggi
RH1	Kerusakan end user	Pencadangan informasi	Preventif	1	5	5	Sedang
RH2	Kerusakan server	Belum ada	Tidak keduanya	2	5	10	Tinggi
RH3		Melindungi dari fisik dan ancaman lingkungan	Preventif	1	4	4	Rendah
RH4	Server down	Pencadangan informasi	Preventif & Protektif	1	3	3	Rendah
RH5	Kehilangan data	Pencadangan informasi	Preventif & Protektif	3	3	9	Tinggi
RH6	Gangguan jaringan	Keamanan informasi selama gangguan	Preventif & Protektif	1	3	3	Rendah
RP1	Developer kurang mampu menangani system crash	Belum ada	Tidak keduanya	2	3	6	Sedang
RP2	Dosen salah menginputkan data	Hak akses	Tidak keduanya	2	4	8	Sedang
RP3	Mahasiswa salah menginputkan data	Belum ada	Tidak keduanya	2	4	8	Tinggi
RP4	Mahasiswa memberikan kunci akses akunnya kepada pihak lain	Belum ada	Tidak keduanya	3	2	6	Sedang

Berikut adalah gambar tingkat kemungkinan risiko yang menggambarkan probabilitas terjadinya risiko terkait penggunaan sistem informasi akademik (SIAKAD) di Universitas XYZ. Tabel ini mencakup rangkuman tingkat kemungkinan risiko dalam kategori yang sudah ditentukan, mulai dari "Sangat Mungkin" hingga "Langka". Dengan rangkuman ini, universitas dapat mengidentifikasi risiko-risiko yang memiliki kemungkinan tinggi untuk terjadi, memungkinkan mereka untuk fokus pada mitigasi risiko yang paling mendesak dan kritis bagi operasional SIAKAD mereka.

Tabel 7. Tingkat kemungkinan risiko

		Kemungkinan				
		Langka	Jarang Terjadi	Memungkinkan	Kemungkinan Besar	Sangat Mungkin
Dampak	Ekstrim	RD2, RH1	RH2	RPS		
	Besar	RD4, RS1, RH3	RS3, RP2, RP3			
	Sedang	RS2, RH4, RH6	RPI	RH5		
	Kecil	RD2, RD3		RP4		
	Tidak Signifikan					

7. *Risk Treatment*

Berikut adalah gambar yang menunjukkan setiap risiko yang telah ditetapkan kategori. Dengan penetapan langkah-langkah pengelolaan risiko, universitas dapat secara sistematis mengurangi dampak risiko-risiko tersebut terhadap operasi dan keandalan SIAKAD, memastikan kelancaran

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 4 Oktober 2024 Hal. 649-656
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

aktivitas akademik dan administratif secara efektif dan efisien [19].

Tabel 8. *Risk treatment*

ID Risk	Accepted?	Risk Treatment Category	Risk Treatment Plan
RD1	Diterima	Accept	Tidak Ada
RD2	Diterima	Accept	Tidak Ada
RD3	Diterima	Accept	Tidak Ada
RD4	Diterima	Accept	Tidak Ada
RS1	Diterima	Accept	Tidak Ada
RS2	Diterima	Accept	Tidak Ada
RS3	Tidak Diterima	Mitigate	Manajemen Kerentanan Teknis
RH1	Diterima	Accept	Tidak Ada
RH2	Tidak Diterima	Mitigate	Persyaratan Keamanan Aplikasi
RH3	Diterima	Accept	Tidak Ada
RH4	Diterima	Accept	Tidak Ada
RH5	Tidak Diterima	Mitigate	Kontrol Akses
RH6	Diterima	Accept	Tidak Ada
RP1	Diterima	Accept	Tidak Ada
RP2	Tidak Diterima	Mitigate	Kontrol Akses
RP3	Tidak Diterima	Mitigate	Persyaratan Keamanan Aplikasi
RP4	Diterima	Accept	Tidak Ada
RP5	Tidak Diterima	Tranfer	Asuransi

8. *Risk Acceptance*

Dari gambar *risk treatment*, dapat disimpulkan bahwa terdapat 12 ID risiko yang diterima dalam pengelolaan risiko pada Sistem Informasi Akademik (SIAKAD) di Universitas XYZ. Risiko-risiko ini termasuk RD1, RD2, RD3, RD4, RS1, RS2, RH1, RH3, RH4, RH6, RP1 dan RP4. Langkah-langkah mitigasi atau penanganan risiko telah ditentukan dan diimplementasikan untuk setiap risiko yang diterima. Namun, terdapat juga 6 ID risiko yang melebihi *level acceptance*, yaitu RS3, RH2, RH5, RP2, RP3, dan RP5. Risiko-risiko ini dianggap memiliki dampak atau kemungkinan terjadi yang melebihi batas yang telah ditetapkan dalam proses evaluasi risiko. Oleh karena itu, untuk risiko-risiko ini telah diberikan *treatment* atau langkah-langkah khusus dalam gambar *risk treatment* [20].

SIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan bahwa pemetaan identifikasi aset awal menghasilkan beberapa aset, yaitu data, perangkat lunak (*software*), perangkat keras (*hardware*), dan sumber daya manusia (*people*). Dari temuan yang terdapat dalam dokumen analisis risiko, terdapat beberapa level risiko yang dikategorikan sebagai rendah, sedang, dan tinggi. Setelah dilakukan evaluasi, nilai risiko tersebut mengalami perubahan. Salah satu risiko dikategorikan sebagai ekstrim meskipun demikian ada beberapa risiko yang tergolong tinggi tetapi telah disusun Rencana Penanganan Risiko (*Risk Treatment Plan*). Yang diharapkan pada evaluasi berikutnya, Universitas XYZ dapat melakukan kontrol yang lebih baik terhadap penelitian ini.

DAFTAR PUSTAKA

[1] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "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," *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, 2019, doi: 10.1016/j.procs.2019.11.234.

[2] D. Fatih and R. F. Aji, "Evaluasi Keamanan Informasi Menggunakan ISO / IEC 27001 : Studi Kasus PT XYZ," vol. 8, pp. 72–84, 2024.

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

[4] Sindi Aprianti, Renny Puspita Sari, and Ibnur Rusi, "Manajemen Risiko Keamanan Simbada Menggunakan Metode NIST SP 800-30 Revisi 1 dan Kontrol ISO/IEC 27001:2013," J. Buana Inform., vol. 14, no. 01, pp. 50–59, 2023, doi: 10.24002/jbi.v14i01.7043..

[5] Tutik, N. Mutiah, and I. Rusi, "Analisis Dan Manajemen Risiko Keamanan Informasi Menggunakan Metode Failure Mode And Effects Analysis (FMEA) Dan ISO/IEC 27001:2013," *Coding J. Komput. dan Apl.*, vol. 10, no. 02, pp. 249–261, 2022.

[6] Syifaurachman and A. Wibowo, "Risk Assessment Related To Privacy Information on Electronic Money Server-Based Using Iso 27001 Iso 27005, Iso 27701," *J. Theor. Appl. Inf. Technol.*, vol. 101, no. 3, pp. 1067–1077, 2023.

[7] T. S. Putri, N. Mutiah, and D. Prawira, "Analisis Manajemen Risiko Keamanan Informasi Menggunakan Nist Cybersecurity Framework dan ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat)," *Coding J. Komput. dan Apl.*, vol. 10, no. 2, pp. 237–248, 2022.

[8] H. Sulaeman, H. P. Utomo, and A. Suryana, "Penilaian Risiko Keamanan Informasi Pada Sistem Informasi Akademik (Siakad) Dengan Menggunakan Framework Nist-Sp 800 30," *Naratif J. Nas. Riset, Apl. dan Tek. Inform.*, vol. 5, no. 2, pp. 171–185, 2023, doi: 10.53580/naratif.v5i2.254.

[9] D. Anggraini and R. Bisma, "Perencanaan Tata Kelola Keamanan Informasi dalam Penerapan Cloud Computing Menggunakan ISO 27001:2013 pada PT.SPINDO,Tbk," *J. Informatics Comput. Sci.*, vol. 3, no. 01, pp. 46–54, 2021, doi: 10.26740/jinacs.v3n01.p46-54.

[10] Gina Cahya Utami, Aden Bahtiar Supramaji, and Khairunnisak Nur Isnaini, "Penilaian Risiko Keamanan Informasi pada Website dengan Metode DREAD dan ISO 27005:2018," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 8, no. 1, pp. 47–56, 2023, doi: 10.32528/justindo.v8i1.219.

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 4 Oktober 2024 Hal. 649-656
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

[11] R. J. Gagas, I. Syah, and F. Febryanto, "Analisis, Evaluasi, Dan Mitigasi Risiko Aset Teknologi Informasi Menggunakan Framework Octave Dan Fmea (Studi Kasus: Unit Pengelola Teknis Teknologi Informasi Dan Komunikasi Universitas Xyz)," *J. Khatulistiwa Inform.*, vol. 9, no. 2, pp. 121–133, 2021, doi: 10.31294/jki.v9i2.11368.

[12] M. Nawir, I. AP, and F. Wajidi, "INTEGRATION OF FRAMEWORK ISO 27001 AND COBIT 2019 IN SMART TOURISM INFORMATION SECURITY PT. YoY INTERNATIONAL MANAGEMENT," *J. Komput. dan Inform.*, vol. 10, no. 2, pp. 122–128, 2022, doi: 10.35508/jicon.v10i2.7985.

[13] M. Amirinnisa1 and R. Bisma2, "Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun," *Jeisbi*, vol. 04, no. 04, pp. 47–58, 2023.

[14] J. Juminovario and E. S. Negara, "Manajemen Risiko Divisi Sistem Informasi Pada Universitas Bina Insan Menggunakan Framework Cobit 5," *CogITo Smart J.*, vol. 8, no. 2, pp. 491–500, 2022, doi: 10.31154/cogito.v8i2.435.491-500.

[15] S. Rif and R. Bisma, "Pembuatan Standard Operating Procedure (SOP) Keamanan Informasi Berdasarkan Framework ISO / IEC 27001: 2013 dan ISO / IEC 27002: 2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun," *JEISBI (Journal Emerg. Inf. Syst. Bus. Intell.*, vol. 01, pp. 43–50, 2020.

[16] D. G. L. W. D et al., "'Hvljq Ri, Qirupdwlrq 6Hfxulw\ 5Lvn 0Dqdjhphqw 8Vlqj, 62, (& Dqg 1,67 63 5Hylvlrq $ &Dvh 6Wxg\ Dw &Rppxqlfdwlrq 'Dwd$Ssolfdwlrqv Ri ;<=, Qvwlwxwh," pp. 3–8.

[17] L. Munaroh, Y. Amrozi, and R. A. Nurdian, "Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013," *Technomedia J.*, vol. 5, no. 2 Februari, pp. 167–181, 2020, doi: 10.33050/tmj.v5i2.1377.

[18] I. P. S. Syahindra, C. Hetty Primasari, and A. Bagas Pradipta Iriantor, "Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi Xyz Menggunakan Indeks Kami Dan Iso 27005: 2011," *J. Teknoinfo*, vol. 16, no. 2, p. 165, 2022, doi: 10.33365/jti.v16i2.1246.

[19] J. Jonny, A. Ambarwati, and C. Darujati, "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005," *Sistemasi*, vol. 10, no. 1, p. 1, 2021, doi: 10.32520/stmsi.v10i1.995.

[20] M. Wasesa, A. Info, C. Resilience, D. Security, and I. S. Control, "Managing Inherent IT Business Risk against Cyber Threats : a Decision Analysis Case Study of an Oil and Gas Company," vol. 5, no. 1, 2024, doi: 10.59395/ijadis.v5i1.1315.