MODEL PRIORITAS MITIGASI RISIKO KEAMANAN INFORMASI SISTEM KEAMANAN AKADEMIK MENGGUNAKAN INTEGRASI AHP-TOPSIS BERBASIS SNI ISO/IEC 27001

Saut Parulian Simatupang, Apriade Voutama
Sistem Informasi, Universitas Singaperbangsa Karawang
Jl.HS. Ronggowaluyo, Karawang, Jawa Barat, Indonesia
Saut.p.simatupang@gmail.com

ABSTRAK

Transformasi digital di perguruan tinggi mendorong adopsi Sistem Informasi Akademik (SIAKAD) yang menyimpan data sensitif. Namun, pendekatan manajemen risiko keamanan informasi yang ada belum menyediakan model terstruktur untuk memprioritaskan mitigasi ancaman. Penelitian ini bertujuan mengembangkan model prioritas mitigasi risiko keamanan informasi pada SIAKAD menggunakan integrasi metode Analytical Hierarchy Process (AHP) dan Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) berbasis SNI ISO/IEC 27001:2022. Penelitian menggunakan pendekatan kuantitatif dengan desain evaluatif melalui studi literatur sistematis dan analisis dokumentasi. Berdasarkan standar SNI ISO/IEC 27001:2022, ditetapkan tiga kriteria (kerahasiaan, integritas, ketersediaan) dan enam alternatif risiko (SQL Injection, Cross-Site Scripting, Brute Force Attack, Denial of Service, Session Hijacking, Insecure Backup). Hasil pembobotan AHP menghasilkan bobot tertinggi pada kerahasiaan (0,539), diikuti integritas (0,297) dan ketersediaan (0,164) dengan Consistency Ratio 0,012 (<0,1). Pemeringkatan TOPSIS menunjukkan SQL Injection sebagai prioritas tertinggi (0,8074), kemudian Session Hijacking (0,6806) dan Insecure Backup (0,5319). Model ini memberikan kontribusi sebagai sistem pendukung keputusan terstruktur yang mengintegrasikan standar keamanan nasional dengan data objektif studi dokumentasi.

Kata kunci : *AHP-TOPSIS, SIAKAD, SNI ISO/IEC 27001, Keamanan Informasi*

1. PENDAHULUAN

Transformasi digital di perguruan tinggi telah menjadikan Sistem Informasi Akademik (SIAKAD) sebagai fondasi utama pengelolaan data pendidikan, mulai dari penerimaan mahasiswa baru hingga layanan akademik [1], [2]. Di balik manfaat efisiensi, SIAKAD menyimpan data sensitif seperti identitas mahasiswa, riwayat akademik, dan transaksi keuangan, sehingga menjadi target utama serangan siber [1]. Ancaman seperti SQL Injection, session hijacking, hingga gangguan infrastruktur kelistrikan tidak hanya mengganggu operasional kampus tetapi juga berpotensi menimbulkan kerugian finansial dan menurunkan kepercayaan pengguna [3].

Berbagai upaya telah dilakukan, mulai dari vulnerability assessment dengan kerangka OWASP dan model DREAD [3], [4] hingga audit kepatuhan berbasis ISO/IEC 27001 [1], [2]. Namun, pendekatan tersebut umumnya berfokus pada pengujian teknis atau audit semata, sehingga memiliki keterbatasan dalam mengintegrasikan dokumentasi kebijakan dan prosedur sebagai cerminan kondisi nyata. Penelitian tentang persepsi mahasiswa [5] masih bersifat deskriptif, sementara metode MCDM seperti AHP dan TOPSIS telah terbukti efektif dalam pemeringkatan risiko [6] namun penerapannya pada SIAKAD dengan data dokumentasi internal masih jarang. Penelitian Primaranti et al. [7] mengakui belum adanya mekanisme prioritas yang sistematis, dan Kumar et al. [8] menekankan pentingnya pengukuran dampak risiko sejak tahap desain. Dengan demikian, kesenjangan yang teridentifikasi adalah belum adanya model yang mengintegrasikan SNI ISO/IEC 27001:2022, data objektif dokumen institusi, dan metode AHP-TOPSIS secara komprehensif.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan menghasilkan sistem pendukung keputusan prioritas mitigasi risiko SIAKAD dengan mengembangkan model yang mengintegrasikan tiga pilar strategis: SNI ISO/IEC 27001:2022 sebagai acuan standar nasional, analisis dokumen internal sebagai basis data objektif, serta metode AHP-TOPSIS untuk menghasilkan urutan penanganan risiko yang presisi melalui pendekatan kuantitatif evaluatif berbasis studi literatur sistematis dan dokumentasi.

2. TINJAUAN PUSTAKA

Tinjauan pustaka ini mencakup konsep, standar, serta metode yang relevan dengan topik penelitian, khususnya terkait manajemen risiko keamanan informasi pada sistem akademik. Selain itu, pada bagian ini juga dipaparkan hasil penelitian terdahulu yang menjadi referensi dan pembanding dalam penyusunan penelitian ini. Dengan adanya tinjauan pustaka, diharapkan dapat memberikan pemahaman yang komprehensif serta memperkuat kerangka pemikiran dalam penelitian yang dilakukan.

.

2.1. SNI ISO/IEC 27001:2022

SNI ISO/IEC 27001:2022 merupakan standar nasional Indonesia yang mengadopsi ISO/IEC 27001:2022 tentang sistem manajemen keamanan

informasi (*Information Security Management System* - ISMS). Standar ini menetapkan persyaratan untuk membangun, menerapkan, memelihara, dan meningkatkan sistem manajemen keamanan informasi secara berkelanjutan [9]. SNI ISO/IEC 27001:2022 menekankan pendekatan berbasis risiko dan menerapkan siklus PDCA (*Plan-Do-Check-Act*) dalam pengelolaan keamanan informasi.

Dalam konteks manajemen risiko, standar ini mengidentifikasi tiga aspek utama yang menjadi dasar penilaian risiko, yaitu:

a. Kerahasiaan (*Confidentiality*)
   Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang;
b. Integritas (*Integrity*)
   Menjamin keakuratan dan kelengkapan informasi serta metode pemrosesannya;
c. Ketersediaan (*Availability*)
   Menjamin bahwa informasi dapat diakses dan digunakan oleh pihak yang berwenang sesuai kebutuhan.

Standar ini menyediakan 93 kontrol keamanan yang dikelompokkan ke dalam empat klausul utama: A.5 (Kebijakan Keamanan Informasi), A.6 (Pengorganisasian Keamanan Informasi), A.7 (Keamanan Sumber Daya Manusia), dan A.8 (Manajemen Aset) hingga A.18 (Kepatuhan) [9].

2.2. Manajemen Risiko Keamanan Informasi SIAKAD

Manajemen risiko keamanan informasi merupakan proses identifikasi, analisis, evaluasi, dan penanganan risiko terhadap aset informasi. Dalam konteks SIAKAD, penelitian Nurbojatmiko et al. [2] melakukan penilaian tingkat kematangan keamanan informasi menggunakan kerangka SSE-CMM (System Security Engineering-Capability Maturity Model) berbasis ISO 27001. Hasil penelitian menunjukkan bahwa domain kontrol akses merupakan domain dengan nilai tertinggi, namun masih diperlukan kebijakan formal untuk memastikan konsistensi penerapan.

Penelitian Dalilah [4] menggunakan model DREAD untuk mengevaluasi risiko keamanan pada SIAKAD Universitas XYZ. Model DREAD menilai risiko berdasarkan lima parameter: Damage Potential, Reproducibility, Exploitability, Affected Users, dan Discoverability. Hasil evaluasi mengidentifikasi SQL Injection dan Session Hijacking sebagai serangan dengan tingkat risiko tertinggi.

Izzani et al. [1] melakukan evaluasi penerapan keamanan informasi pada SIAKAD Universitas Ibrahimy menggunakan ISO/IEC 27001:2022. Penelitian ini menemukan bahwa tingkat kesesuaian penerapan keamanan informasi pada SIAKAD mencapai 86%, namun masih terdapat kesenjangan pada aspek kebijakan keamanan dan prosedur pencadangan data.

2.3. Analytical Hierarchy Process (AHP)

AHP adalah metode pengambilan keputusan multi kriteria yang dikembangkan oleh Thomas L. Saaty [10]. Metode ini didasarkan pada penyusunan hierarki, penilaian perbandingan berpasangan, dan uji konsistensi logis. Keunggulan AHP terletak pada kemampuannya untuk mengubah penilaian kualitatif menjadi nilai kuantitatif yang konsisten. Tahapan utama AHP meliputi:

a. Dekomposisi
   Menyusun permasalahan ke dalam struktur hierarki (goal, kriteria, alternatif).
b. Perbandingan Berpasangan
   Menentukan tingkat kepentingan relatif antar elemen menggunakan skala 1-9.
c. Perhitungan Bobot Prioritas
   Melakukan normalisasi matriks dan menghitung vektor prioritas;
d. Uji Konsistensi
   Menghitung *Consistency Ratio* (CR) untuk memastikan konsistensi penilaian (CR ≤ 0,1).

2.4. Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)

TOPSIS adalah metode MCDM yang dikembangkan oleh Hwang dan Yoon. Metode ini bekerja berdasarkan konsep bahwa alternatif terbaik harus memiliki jarak terpendek terhadap solusi ideal positif dan jarak terpanjang terhadap solusi ideal negatif [12]. Tahapan perhitungan TOPSIS meliputi:

a. Membangun Matriks Keputusan
   Menyusun nilai setiap alternatif pada setiap kriteria.
b. Normalisasi Matriks
   Menghilangkan perbedaan satuan dan skala antar kriteria.
c. Membangun Matriks Ternormalisasi Terbobot
   Mengalikan matriks ternormalisasi dengan bobot kriteria.
d. Menentukan Solusi Ideal Positif dan Negatif
   Mengidentifikasi nilai terbaik dan terburuk setiap kriteria.
e. Menghitung Jarak Terhadap Solusi Ideal
   Menggunakan *Euclidean distance*.
f. Menghitung Nilai Kedekatan Relatif
   Menentukan preferensi akhir setiap alternatif.

Integrasi AHP-TOPSIS telah banyak diterapkan dalam berbagai bidang, termasuk keamanan siber dan sistem informasi. Chahid *et al.* [6] menggunakan integrasi AHP-TOPSIS dan ITIL v4 untuk memperkuat ketahanan siber di universitas Maroko, menunjukkan bahwa pendekatan MCDM efektif dalam mengoptimalkan alokasi sumber daya keamanan.

2.5. Penelitian Terdahulu

Beberapa penelitian telah dilakukan terkait evaluasi risiko keamanan informasi pada sistem akademik. Kusnandar menggunakan metode FMEA (Failure Mode and Effects Analysis) berbasis ISO

27001 untuk mengukur tingkat risiko keamanan informasi pada suatu instansi. Penelitian ini menghasilkan identifikasi mode kegagalan prioritas yang memerlukan penanganan segera [13].

Primaranti menganalisis risiko keamanan informasi pada website repository digital library menggunakan kerangka ISO/IEC 27001 dan 27002. Penelitian ini menekankan pentingnya tindak lanjut mitigasi setelah identifikasi kerentanan, namun belum menyediakan mekanisme prioritas yang sistematis [7].

Muhammad Rafi Wijaya membahas manajemen risiko keamanan siber dalam implementasi teknologi 5G di universitas, menekankan pentingnya pelatihan keamanan siber bagi seluruh sivitas akademika dalam menghadapi ancaman yang semakin kompleks [14].

Sikman mengembangkan model penilaian aspek terukur ISMS (Information Security Management System) di pendidikan tinggi menggunakan logika fuzzy. Penelitian ini memperkuat pentingnya pendekatan terstruktur dalam mengevaluasi kematangan keamanan informasi [15].

3. METODE PENELITIAN

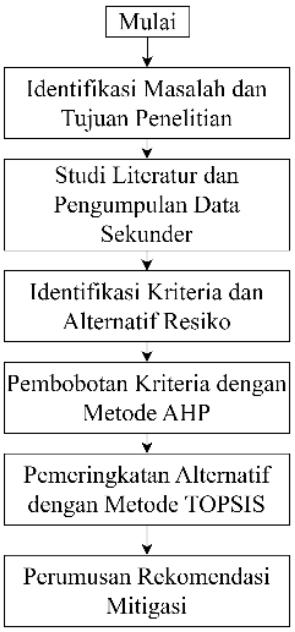
Penelitian ini menerapkan pendekatan kuantitatif *Multi Cirteria Decision Making* (MCDM) dengan mengintegrasikan metode AHP dan TOPSIS. Pendekatan ini memungkinkan proses pengambilan keputusan yang lebih terstruktur, mengurangi subjektivitas, dan menghasilkan peringkat prioritas yang konsisten.

3.1. Desain Penelitian

Penelitian ini menggunakan desain penelitian evaluative dengan pendekatan studi literatur sistematis. Objek penelitian adalah Sistem Informasi Akademik (SIAKAD) pada perguruan tinggi di Indonesia secara umum, tanpa terbatas pada institusi tertentu. Tahapan penelitian meliputi: (1) identifikasi masalah dan tujuan penelitian, (2) studi literatur dan pengumpulan data sekunder, (3) identifikasi kriteria dan alternatif risiko, (4) pembobotan kriteria dengan metode AHP, (5) pemeringkatan alternatif risiko dengan metode TOPSIS, dan (6) perumusan rekomendasi mitigasi.

3.2. Tahapan Penelitian

Penelitian ini dilaksanakan melalui enam tahapan sistematis sebagaimana diilustrasikan pada Gambar 1. Tahapan dimulai dengan identifikasi masalah dan tujuan penelitian untuk menemukan kesenjangan serta menetapkan arah penelitian, dilanjutkan dengan studi literatur dan pengumpulan data sekunder melalui telaah pustaka dan analisis dokumentasi untuk membangun landasan teoritis dan empiris. Selanjutnya dilakukan identifikasi kriteria dan alternatif risiko berdasarkan SNI ISO/IEC 27001:2022 dan temuan penelitian terdahulu, kemudian pembobotan kriteria dengan metode AHP untuk menentukan tingkat kepentingan relatif setiap kriteria, diikuti dengan pemeringkatan alternatif menggunakan metode TOPSIS untuk menghasilkan urutan prioritas risiko, dan diakhiri dengan perumusan rekomendasi mitigasi yang terstruktur dan aplikatif bagi pengelola SIAKAD.



Gambar 1. Tahapan penelitian

Penelitian ini dilaksanakan melalui enam tahapan sistematis sebagaimana diilustrasikan pada Gambar 1. Tahapan dimulai dengan identifikasi masalah dan tujuan penelitian untuk menemukan kesenjangan serta menetapkan arah penelitian, dilanjutkan dengan studi literatur dan pengumpulan data sekunder melalui telaah pustaka dan analisis dokumentasi untuk membangun landasan teoritis dan empiris. Selanjutnya dilakukan identifikasi kriteria dan alternatif risiko berdasarkan SNI ISO/IEC 27001:2022 dan temuan penelitian terdahulu, kemudian pembobotan kriteria dengan metode AHP untuk menentukan tingkat kepentingan relatif setiap kriteria, diikuti dengan pemeringkatan alternatif menggunakan metode TOPSIS untuk menghasilkan urutan prioritas risiko, dan diakhiri dengan perumusan rekomendasi mitigasi yang terstruktur dan aplikatif bagi pengelola SIAKAD.

3.3. Metode Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan melalui studi literatur dan dokumentasi tanpa melibatkan pengumpulan data primer seperti wawancara atau survei lapangan. Pendekatan ini dipilih untuk menghasilkan model yang berbasis pada data objektif dari sumber-sumber terpercaya.

a. Studi Literatur
   Studi pustaka dilakukan sebagai langkah awal untuk memahami konsep, teori, dan penelitian terdahulu yang relevan. Literatur yang dikaji meliputi Standar keamanan informasi SNI ISO/IEC 27001:2022 sebagai acuan utama [9], konsep dan implementasi metode AHP dan

TOPSIS serta integrasi keduanya dan penelitian terkait evaluasi risiko, analisis kerentanan, dan persepsi pengguna terhadap keamanan sistem informasi akademik.

b. Studi Dokumentasi
Studi dokumentasi dilakukan dengan menganalisis dokumen-dokumen sekunder yang relevan dengan keamanan sistem informasi akademik di perguruan tinggi, mengikuti pendekatan yang digunakan dalam penelitian evaluasi SIAKAD sebelumnya [1], [7]. Dokumen yang dianalisis mencakup publikasi ilmiah yang memuat temuan empiris mengenai kerentanan dan risiko pada SIAKAD, laporan dan dokumentasi publik seperti kebijakan keamanan informasi yang dipublikasikan, dokumen SNI ISO/IEC 27001:2022 dan peraturan terkait keamanan informasi di lingkungan pendidikan tinggi. Data yang diperoleh dari studi dokumentasi digunakan untuk mengidentifikasi alternatif risiko yang relevan dengan konteks SIAKAD, seperti SQL Injection, Cross-Site Scripting, *Brute Force Attack*, *Denial of Service*, *Session Hijacking*, dan kerentanan keamanan lainnya yang umum ditemukan.

3.4. Metode Analytical Hierarchy Process (AHP)

Metode AHP merupakan pendekatan pengambilan keputusan multi kriteria yang dikembangkan oleh Thomas L. Saaty [10]. Metode ini didasarkan pada penyusunan hierarki, penilaian perbandingan berpasangan, dan uji konsistensi logis. Implementasi metode ini mengikuti langkah-langkah sistematis sebagai berikut.

3.5. Dekomposisi Masalah

Tahap awal metode AHP adalah dekomposisi, yakni menguraikan permasalahan ke dalam struktur hierarki yang logis. Struktur tersebut disusun secara bertingkat, mulai dari level 1 (Goal), prioritas mitigasi risiko keamanan informasi SIAKAD, Level 2 (Kriteria), yaitu kerahasiaan, integritas, ketersediaan, Level 3 (Alternatif) : enam risiko keamanan yang telah diidentifikasi. Penyusunan hierarki ini bertujuan untuk memecah permasalahan kompleks menjadi komponen-komponen yang lebih sederhana sehingga memudahkan proses penilaian dan analisis.

3.6. Perbandingan Berpasangan

Penilaian dilakukan melalui perbandingan berpasangan (*pairwise comparison*) untuk menentukan tingkat kepentingan relatif antar-elemen pada level yang sama. Penilaian ini dilakukan dengan membandingkan satu elemen terhadap elemen lainnya berdasarkan kontribusinya terhadap elemen di level atasnya. Konversi persepsi kualitatif menjadi angka kuantitatif menggunakan skala preferensi Saaty [10] yang disajikan pada Tabel 1**.**

Tabel 1. Skala Preferensi Saaty

Sintaks Pembanding	Nilai
Sangat diutamakan	9
Lebih menuju sangat diutamakan	8
Lebih diutamakan	7
Diutamakan menuju lebih diutamakan	6
Diutamakan	5
Cukup menuju diutamakan	4
Cukup Diutamakan	3
Setara menuju cukup diutamakan	2
Setara	1

Dari Tabel 1 dapat dilihat bahwa skala preferensi Saaty memberikan rentang nilai 1 hingga 9 yang merepresentasikan tingkat kepentingan relatif antara dua elemen. Semakin tinggi nilai, semakin dominan elemen yang dibandingkan.

$$\mathrm{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1j} \\ a_{21} & a_{22} & \dots & a_{2j} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} \end{bmatrix} \quad (1)$$

Dimana a_1 adalah nilai preferensi elemen i terhadap elemen j. Setelah seluruh nilai preferensi sudah diubah ke dalam matriks perbandingan berpasangan, langkah selanjutnya adalah melakukan perhitungan bobot setiap prioritas. Proses ini melibatkan normalisasi setiap kolom matriks dan perhitungan nilai rata-rata baris untuk memperoleh vektor prioritas.

3.7. Perhitungan Bobot Prioritas

Setelah seluruh nilai preferensi dimasukkan ke dalam matriks perbandingan berpasangan, langkah selanjutnya adalah menghitung bobot setiap prioritas. Proses ini melibatkan normalisasi setiap kolom matriks dan perhitungan nilai rata-rata baris untuk memperoleh vektor prioritas.

$$P_j = \sum_{i=1}^{n} a_{ij} \ , j = 1,2, \dots, n \quad (2)$$

Bobot yang dihasilkan merupakan representasi numerik dari signifikansi masing-masing kriteria, yang nantinya akan menjadi landasan utama dalam menentukan urutan prioritas pada tahap pengambilan keputusan akhir.

3.8. Uji Konsistensi

Uji konsistensi dilakukan untuk memastikan bahwa penilaian perbandingan bersifat konsisten dengan menghitung Consistency Ratio (CR).

$$\mathrm{CI} = ((\lambda\mathrm{maks} - \mathrm{n})/(\mathrm{n} - 1)) \quad (3)$$

Dimana λmaks adalah nilai eigen maksimum dan n adalah jumlah kriteria. Selanjutnya, CR dihitung dengan rumus:

$$\mathrm{CR} = (\mathrm{CI}/\mathrm{RI}) \quad (4)$$

Dimana indeks rasio (RI) dapat dilihat dalam tabel berikut.

Tabel 2. Alternatif Risiko Keamanan SIAKAD

Ukuran Matriks	Nilai IR
1,2	0
3	0,58
4	0,90
5	1,12
6	1,24
7	1,32
8	1,41
9	1,45
10	1,49
1,2	0

Hasil dinyatakan konsisten jika CR ≤ 0,1. Bobot kriteria yang dihasilkan dari metode AHP akan digunakan sebagai input dalam perhitungan TOPSIS.

3.9. Metode TOPSIS

Metode TOPSIS digunakan untuk merangking alternatif risiko berdasarkan bobot kriteria yang telah diperoleh dari AHP. Tahap pertama adalah membangun matriks keputusan X berukuran 6x3 yang merepresentasikan 6 alternatif risiko dan 3 kriteria penilaian. Nilai merepresentasikan tingkat dampak risiko ke-i terhadap kriteria ke-j. Nilai ini merupakan skor kuantitatif yang diperoleh dari sintesis temuan studi dokumentasi, dengan skala 1 untuk dampak sangat rendah hingga 5 untuk dampak sangat tinggi. Matriks keputusan kemudian dinormalisasi menggunakan rumus:

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \quad (5)$$

Nilai r_ij adalah elemen matriks ternormalisasi, x_ij adalah nilai dampak risiko ke-i pada kriteria ke-j, i adalah indeks untuk alternatif (1 sampai 6), dan j adalah indeks untuk kriteria (1 sampai 3). Proses normalisasi bertujuan untuk menghilangkan perbedaan satuan dan skala antar kriteria. Selanjutnya, matriks ternormalisasi terbobot dibangun dengan mengalikan matriks ternormalisasi dengan bobot kriteria yang diperoleh dari hasil AHP menggunakan rumus:

$$y_{ij} = w_i r_{ij} \quad (6)$$

Nilai y_ij adalah elemen matriks ternormalisasi terbobot w_i adalah bobot kriteria ke-i yang diperoleh dari hasil AHP, dan r_ij adalah elemen matriks ternormalisasi. Hasil perkalian ini menghasilkan matriks baru yang telah mempertimbangkan tingkat kepentingan masing-masing kriteria. Setelah itu kita akan menentukan sebuah matriks solusi ideal positif dan negatif . Solusi ideal positif (A+) dan solusi ideal negatif (A-) ditentukan berdasarkan nilai terbaik dan terburuk pada setiap kriteria.

$$A^+ = y_1^+, y_2^+, \ldots\ldots\ldots, y_n^+ \quad (7)$$

$$A^{\pm} = y_1^-, y_2^-, \ldots\ldots\ldots, y_n^- \quad (8)$$

Notasi A+ menyatakan himpunan solusi ideal positif yang terdiri dari y_1^+, y_2^+, hingga y_n^+, dimana setiap y_j^+ merupakan nilai maksimum dari kolom ke-j pada matriks terbobot. Notasi A- menyatakan himpunan solusi ideal negatif yang terdiri dari y_1^-, y_2^-, hingga y_n^-, dimana setiap y_j^- merupakan nilai minimum dari kolom ke-j pada matriks terbobot. Jarak setiap alternatif terhadap solusi ideal positif dan solusi ideal negatif dihitung menggunakan Euclidean distance dengan rumus:

$$D_i^+ = \sqrt{\sum_{j=1}^{n} (y_{ij} - y_j^+)^2} \quad (9)$$

$$D_i^- = \sqrt{\sum_{j=1}^{n} (y_{ij} - y_j^-)^2} \quad (10)$$

Nilai D_i^+ adalah jarak alternatif ke-i terhadap solusi ideal positif, yang diperoleh dari akar jumlah kuadrat selisih antara nilai y_{ij} dan y_j^+ untuk semua kriteria. Nilai y_{ij} merupakan nilai terbobot alternatif ke-i pada kriteria ke-j, sedangkan y_j^+ adalah nilai solusi ideal positif pada kriteria ke-j. Nilai D_i^- adalah jarak alternatif ke-i terhadap solusi ideal negatif, yang diperoleh dari akar jumlah kuadrat selisih antara nilai y_{ij} dan y_j^- untuk semua kriteria, dimana y_j^- adalah nilai solusi ideal negatif pada kriteria ke-j. Indeks i menunjukkan alternatif ke-1 hingga ke-6, sedangkan j menunjukkan kriteria ke-1 hingga ke-3.

Langkah terakhir adalah menghitung nilai relatif kedekatan untuk setiap alternatif terhadap solusi ideal positif dengan rumus:

$$c_i^+ = \frac{s_i^-}{(s_i^- - s_i^+)} \quad (11)$$

Nilai C_i merupakan nilai preferensi atau kedekatan relatif alternatif ke-i terhadap solusi ideal positif, dengan rentang nilai antara 0 hingga 1. Nilai S_i^- adalah jarak alternatif ke-i terhadap solusi ideal negatif dan S_i^+ adalah jarak alternatif ke-i terhadap solusi ideal positif, dimana i adalah indeks untuk alternatif ke-1 hingga ke-6.

Setelah nilai preferensi untuk setiap alternatif diperoleh, langkah selanjutnya adalah menentukan pemeringkatan alternatif. Alternatif diurutkan berdasarkan nilai C_i dari yang terbesar hingga yang terkecil. Alternatif dengan nilai C_i terbesar merupakan alternatif terbaik dan menjadi prioritas utama untuk dilakukan mitigasi. Hal ini dikarenakan rumus C_i mengindikasikan bahwa semakin kecil jarak alternatif terhadap solusi ideal positif (S_i^+) dan semakin besar jarak alternatif terhadap solusi ideal negatif (S_i^-), maka semakin tinggi nilai preferensi suatu alternatif. Dengan demikian, alternatif yang memiliki nilai preferensi tertinggi dianggap sebagai prioritas utama dalam mitigasi risiko keamanan sistem informasi akademik menggunakan metode TOPSIS

4. HASIL DAN PEMBAHASAN

Berdasarkan SNI ISO/IEC 27001:2022 dan berbagai penelitian terdahulu, ditetapkan tiga kriteria utama yang menjadi dasar penilaian risiko keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan sistem. Berdasarkan dokumentasi terhadap publikasi ilmiah yang memuat temuan

mengenai kerentanan pada sistem informasi akademik, diidentifikasi enam alternatif risiko yang paling relevan.

Tabel 3. Alternatif Risiko Keamanan SIAKAD

Kode	Alternatif Risiko
A1	SQL Injection
A2	Cross Site Scripting
A3	Brute Force Attack
A4	Denial Of Service
A5	Session Hijacking
A6	Insecure Backup

Pembobotan kriteria dilakukan melalui penilaian oleh para ahli yang memahami manajemen keamanan informasi dan sistem informasi akademik. Hasil rekapitulasi penilaian para ahli dirata-ratakan menggunakan *geometric mean* untuk memperoleh matriks perbandingan berpasangan tunggal.

Tabel 4. Matriks Perbandingan Berpasangan Antar Kriteria

Kriteria	Kerahasiaan	Integritas	Ketersediaan
Kerahasiaan	1	2,5	3
Intergritas	0,4	1	2
Ketersediaan	0,33	0,5	1

Setelah dilakukan normalisasi matriks dan perhitungan vektor prioritas, diperoleh bobot masing-masing kriteria. Uji konsistensi menunjukkan nilai *Consistency Ratio* (CR) sebesar 0,012, yang berarti lebih kecil dari 0,10 sehingga dinyatakan konsisten.

Tabel 5. Bobot Kriteria Hasil Perhitungan AHP

Kriteria	Bobot	Prioritas
Kerahasiaan	0,539	1
Intergritas	0,297	2
Ketersediaan	0,3	3

Hasil pembobotan menunjukkan aspek kerahasiaan menjadi kriteria dengan prioritas tertinggi, diikuti oleh integritas dan ketersediaan. Hal ini menunjukkan perlindungan data pribadi dan informasi sensitif menjadi perhatian utama dalam pengelolaan keamanan informasi di perguruan tinggi. Setelah bobot kriteria didapatkan, selanjutnya dilakukan pemeringkatan pada enam alternatif risiko menggunakan metode TOPSIS. Matriks keputusan awal yang berisi nilai dampak setiap alternatif risiko terhadap masing-masing kriteria disajikan pada tabel berikut.

Tabel 6. Matriks Keputusan Awal

Kode	Kerahasiaan	Integritas	Ketersediaan
A1	5	5	3
A2	4	3	2
A3	4	4	3
A4	2	3	5
A5	5	4	3
A6	4	5	4

Matriks keputusan kemudian dinormalisasi dan dikalikan dengan bobot kriteria hasil AHP. Selanjutnya, dihitung jarak setiap alternatif terhadap solusi ideal positif dan negatif, serta nilai kedekatan relatif (Ci) untuk setiap alternatif.

Tabel 7. Hasil Perhitungan TOPSIS

Kode	Jarak ke A+	Jarak ke A-	Nilai Preferensi	Peringkat
A1	0,0214	0,0897	0,8074	1
A2	0,0358	0,0763	0,6806	2
A3	0,0521	0,0592	0,5319	3
A4	0,0689	0,0425	0,3815	4
A5	0,0852	0,0314	0,2693	5

SQL Injection sebagai prioritas utama (0,8074) menunjukkan bahwa kerentanan pada lapisan basis data merupakan ancaman paling kritis. Temuan ini sejalan dengan penelitian yang mengidentifikasi SQL Injection sebagai kerentanan dengan tingkat risiko tertinggi [3], [4]. Dalam konteks SNI ISO/IEC 27001:2022, risiko ini berkaitan erat dengan prinsip kerahasiaan dan integritas. Eksploitasi celah ini dapat mengakibatkan kebocoran data sensitif dan modifikasi nilai akademik.

Session Hijacking menempati peringkat kedua (0,6806). Risiko ini memungkinkan penyerang mengambil alih sesi pengguna yang sah. Penelitian sebelumnya mengidentifikasi session hijacking sebagai serangan dengan tingkat risiko tinggi pada SIAKAD [4]. Dalam SNI ISO/IEC 27001:2022, risiko ini berkaitan dengan klausul A.9 (*Access control*).

Insecure Backup menempati peringkat ketiga (0,5319), mengindikasikan bahwa meskipun sering terabaikan, dampaknya terhadap ketersediaan dan integritas data sangat signifikan [7]. Risiko ini terkait dengan klausul A.8 (*Manajemen Aset*) dan A.12 (*Keamanan Operasional*). Kontribusi model MCDM terstruktur dalam penelitian ini adalah menghadirkan pendekatan yang mengintegrasikan aspek normatif standar keamanan dengan data objektif dari studi dokumentasi. Pendekatan ini melengkapi metode yang ada sebelumnya yang hanya berfokus pada aspek teknis semata [6].

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengembangkan model prioritas mitigasi risiko keamanan informasi pada SIAKAD melalui integrasi metode AHP dan TOPSIS berbasis SNI ISO/IEC 27001:2022. Model yang dihasilkan mampu mensinergikan tiga pilar strategis, yaitu keselarasan dengan standar keamanan nasional, pemanfaatan data objektif dari studi dokumentasi, serta penerapan metode MCDM yang terstruktur. Berdasarkan hasil pembobotan kriteria, aspek kerahasiaan menjadi prioritas tertinggi dengan bobot 0,539. Hasil pemeringkatan menunjukkan SQL Injection sebagai prioritas mitigasi tertinggi (0,8074), diikuti oleh Session Hijacking (0,6806) dan Insecure Backup (0,5319). Penelitian selanjutnya disarankan untuk melakukan validasi empiris model melalui studi

kasus pada institusi yang menerapkan SNI ISO/IEC 27001:2022 secara penuh serta mengintegrasikan data *real-time* dari sistem deteksi intrusi untuk meningkatkan akurasi dan dinamika pemeringkatan risiko..

DAFTAR PUSTAKA

[1] M. Izzani, N. Nellatul, A. Ismatul, and A. Hamdani, "Evaluasi penerapan keamanan informasi pada SIAKAD Universitas Ibrahimy berbasis ISO/IEC 27001:2022," Jurnal Ilmiah Sistem Informasi, vol. 5, no. 1, pp. 175–185, 2026.

[2] A. Nurbojatmiko, Q. Aini, N. C. Wasiqi, M. F. Alfajri, Z. Ulinnuha, Y. K. Purwati, I. K. Ayu, and N. A. Yasmin, "Risk assessment maturity level of academic information system using ISO 27001 system security engineering-capability maturity model," Journal of Applied Engineering and Technological Science, vol. 5, no. 2, pp. 941–954, 2024.

[3] Y. Mulyanto, E. Haryanti, and J. Jumirah, "Analisis keamanan website SMAN 1 Sumbawa menggunakan metode vulnerability assessment," Jurnal Informatika Teknologi dan Sains, vol. 3, no. 3, pp. 394–400, 2021.

[4] D. Dalilah, "Evaluasi risiko keamanan menggunakan model DREAD terhadap sistem informasi akademik Universitas XYZ," JUSIM (Jurnal Sistem Informasi Musirawas), vol. 7, no. 1, pp. 68–80, 2022.

[5] A. S. Adlianto, D. K. Dali, F. Zahra, and S. Muhammad, "Analisis persepsi mahasiswa fakultas ilmu komputer terhadap keamanan sistem informasi akademik di Universitas Bhayangkara Jakarta Raya," Journal of Informatic and Information Security, vol. 5, no. 2, pp. 223–234, 2025.

[6] A. Chahid, S. Ahriz, K. El Guemmat, and K. Mansouri, "Strengthening resilience against cyberattacks in Moroccan Universities through AHP, TOPSIS, and ITIL v4," Indonesian Journal of Electrical Engineering and Computer Science, vol. 37, no. 3, pp. 1999–2008, 2025.

[7] J. Primaranti, A. F. Setyowardhani, I. Nurlela, V. Ghrandiaz, and Y. Yulhendri, "Analisis risiko keamanan informasi website repository digital library menggunakan framework ISO/IEC 27001 & 27002: Studi kasus perguruan tinggi X," Jurnal Riset Multidisiplin dan Inovasi Teknologi, vol. 2, no. 1, pp. 327–373, 2023.

[8] R. Kumar, S. A. Khan, and R. A. Khan, "Managing security-risks for improving security-durability of institutional web applications," Computers, Materials & Continua, vol. 66, no. 2, pp. 1857–1872, 2020.

[9] Badan Standardisasi Nasional, *SNI ISO/IEC 27001:2022: Keamanan informasi, keamanan siber, dan proteksi privasi Sistem manajemen keamanan informasi Persyaratan*. Jakarta: BSN, 2023.

[10] T. L. Saaty, "Decision making with the analytic hierarchy process," International Journal of Services Sciences, vol. 1, no. 1, pp. 83–98, 2008.

[11] G. Z. A. Arif and R. Sulaiman, "Integrasi metode AHP-TOPSIS dalam pemeringkatan bank digital di Indonesia," MATHunesa: Jurnal Ilmiah Matematika, vol. 11, no. 2, pp. 199–208, 2023.

[12] L. Šikman, T. Latinović, N. Sarajlić, B. Vranjes, L. Figun, and A. Gaćina, "Model for assessing measurable aspects of information security in higher education," Comptes Rendus de l'Académie Bulgare des Sciences, vol. 78, no. 7, pp. 1–12, 2025.

[13] N. Irawati, A. B. Susanto, and A. K. Rivai, "Studi implementasi SNI ISO/IEC 27001:2022 untuk manajemen risiko data center BBMKG Wilayah II," Journal of Information Technology and Computer Science, vol. 9, no. 1, pp. 1–8, 2024.

[14] M. R. Wijaya, D. Setiawan, M. A. Hermawan, and N. S. Adjhari, "Manajemen risiko keamanan siber dalam implementasi teknologi 5G di Universitas Bhayangkara Jakarta Raya," Journal of Informatic and Information Security, vol. 5, no. 2, pp. 119–132, 2025.

[15] A. Kusnandar, A. F. Rochim, and V. Gunawan, "Pengukuran tingkat risiko dan keamanan informasi menggunakan metode FMEA berbasis ISO/IEC 27001 pada Instansi XYZ untuk keamanan sistem informasi," Jurnal Sistem Informasi Bisnis, vol. 14, no. 4, pp. 375–384, 2024.