Jumistik
E-ISSN: 2964-3953 P-ISSN: 2964-3988
Jurnal Manajemen Informatika, Sistem Informasi dan Teknologi Komputer

Vol.5 No.1 Juni 2026
Hal 778-785
Https://ojs.amiklps.ac.id

MANAJEMEN RISIKO SISTEM INFORMASI PORTAL AKADEMIK *NEW STUDENT* UIGM MENGGUNAKAN METODE ISO 27005

Nining Ariati[1]*, Annisa Octhania[2], Salsyahbilla Aulia[3], Muthiah Tsabitah Sujana[4], Yuni Agita[5]

Sistem Informasi Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri
E-mail: nining@uigm.ac.id[1]*, 2023210034@student.uigm.ac.id[2], 2023210032@student.uigm.ac.id[3], 2023210025@student.uigm.ac.id[4], 2023210036@student.uigm.ac.id[5]

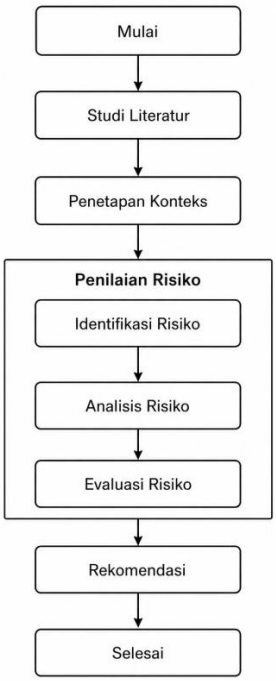
INFO ARTIKEL

Sejarah Artikel
Diterima : 30/04/2026
Direvisi : 11/05/2026
Diterbitkan : 01/06/2026

***Corresponding author**
nining@uigm.ac.id

DOI: 10.70247/jumistik.v5i1.291

GRAPHICAL ABSTRACT



ABSTRACT

The development of information technology in higher education has encouraged the use of academic portals to support academic and administrative activities. The New Student Academic Portal of Universitas Indo Global Mandiri (UIGM) is used for course registration (KRS), viewing class schedules, checking study results, and administrative payments. However, there are still risks such as system disruptions, errors during course registration, student data leakage, and slow system response. This study aims to analyze information security risk management in the New Student Academic Portal of UIGM using the ISO 27005 method. This research uses a descriptive qualitative method through observation, questionnaire distribution, and literature study. The results show that there are seven main risks, with three classified as high-level risks: frequent system disruptions, errors during course registration, and student data leakage. Therefore, increasing server capacity, strengthening access control, regular data backup, and system monitoring are necessary to improve the security and reliability of the academic portal.

***Keywords**: Risk Management, Information Security, Academic Portal, ISO 27005, Academic Information System*

ABSTRAK

Perkembangan teknologi informasi di perguruan tinggi mendorong penggunaan portal akademik untuk mendukung kegiatan akademik dan administrasi. Portal Akademik *New Student* Universitas Indo Global Mandiri (UIGM) digunakan untuk pengisian Kartu Rencana Studi (KRS), melihat jadwal kuliah, memeriksa hasil studi, serta pembayaran administrasi. Namun, masih terdapat risiko seperti gangguan sistem, error saat pengisian KRS, kebocoran data mahasiswa, dan lambatnya respons sistem. Penelitian ini bertujuan untuk menganalisis manajemen risiko keamanan informasi pada Portal Akademik *New Student* UIGM menggunakan metode ISO 27005. Penelitian ini menggunakan metode deskriptif kualitatif melalui observasi, penyebaran kuesioner, dan studi literatur. Hasil penelitian menunjukkan terdapat tujuh risiko utama, dengan tiga risiko berkategori tinggi yaitu gangguan sistem, error saat pengisian KRS, dan kebocoran data mahasiswa. Oleh karena itu, diperlukan peningkatan kapasitas *server*, penguatan kontrol akses, *backup* data rutin, dan *monitoring* sistem untuk meningkatkan keamanan serta keandalan portal akademik.

Kata kunci: Manajemen Risiko, Keamanan Informasi, Portal Akademik, ISO 27005, Sistem Informasi Akademik.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam dua dekade terakhir telah membawa perubahan fundamental dalam cara organisasi merencanakan, mengelola, dan memanfaatkan sumber daya bisnisnya, termasuk di dunia pendidikan [1]. Perubahan ini terlihat jelas pada perguruan tinggi yang kini sangat bergantung pada sistem informasi berbasis web dalam mendukung aktivitas akademik dan administrasi. Portal akademik berbasis web memberikan akses informasi yang lebih mudah, akurat, dan cepat bagi mahasiswa, dosen, dan staf [2]. Kondisi ini menunjukkan bahwa keberadaan teknologi informasi telah menjadi bagian yang tidak terpisahkan dari lingkungan pendidikan tinggi.

Salah satu bentuk penerapannya adalah Portal Akademik *New Student* Universitas Indo Global Mandiri (UIGM) yang memiliki peran penting sebagai sarana utama bagi mahasiswa dalam mengakses berbagai kebutuhan akademik. Melalui sistem ini, mahasiswa dapat melakukan pengisian Kartu Rencana Studi (KRS), melihat jadwal perkuliahan, memeriksa hasil studi, serta mengakses informasi akademik lainnya. Selain itu, sistem ini juga digunakan untuk proses pembayaran administrasi dan layanan awal perkuliahan lainnya secara terintegrasi, sehingga membantu mahasiswa dalam menjalankan aktivitas akademik secara lebih mudah dan terstruktur. Keberadaan sistem yang baik mendukung efektivitas pengelolaan data serta meningkatkan kualitas pelayanan akademik di lingkungan perguruan tinggi [3].

Namun, di balik pemanfaatan portal akademik tersebut, terdapat berbagai risiko yang perlu diperhatikan. Jika perguruan tinggi tidak dapat mengidentifikasi sumber ancaman, maka penerapan portal akademik dapat menimbulkan berbagai risiko [4]. Berdasarkan hasil kuesioner awal, sebagian besar pengguna menilai bahwa portal akademik *New Student* UIGM sudah cukup baik dalam mendukung layanan akademik, terutama pada aspek kemudahan akses dan keamanan data. Namun, masih ditemukan beberapa kendala seperti sistem yang sering mengalami gangguan saat digunakan, portal yang belum sepenuhnya berjalan tanpa error, serta kecepatan respons yang belum optimal.

Seiring dengan kemajuan teknologi, risiko terhadap keamanan informasi juga meningkat secara signifikan. Ancaman seperti kebocoran data, serangan siber, penyalahgunaan akses, gangguan *server*, hingga kerentanan teknis menjadi tantangan utama yang dapat mengganggu keberlangsungan operasional organisasi [5]. Kondisi ini menunjukkan bahwa pengelolaan risiko pada portal akademik menjadi hal yang sangat penting untuk menjaga keamanan, keandalan, dan keberlanjutan layanan akademik. Data yang tersimpan dalam portal akademik mencakup informasi sensitif seperti identitas mahasiswa, dokumen akademik, hingga data pembayaran yang harus dijaga kerahasiaan, integritas, dan ketersediaannya agar tidak menimbulkan kerugian bagi institusi maupun pengguna.

Manajemen risiko sistem informasi menjadi langkah penting untuk memastikan keamanan dan kestabilan portal akademik di perguruan tinggi. Identifikasi serta pengelolaan risiko perlu dilakukan agar sistem dapat berjalan secara optimal dan mampu mendukung seluruh proses akademik maupun administrasi secara efektif. Manajemen risiko merupakan upaya yang dilakukan untuk mengendalikan kemungkinan terjadinya masalah yang dapat menghambat jalannya suatu sistem, sehingga kualitas layanan tetap terjaga. Proses ini bertujuan untuk meminimalkan potensi hasil yang tidak diinginkan dari aktivitas dan keputusan sehari-hari [6]. Dalam konteks portal akademik, penerapan manajemen risiko membantu menjaga keamanan informasi, ketersediaan sistem, serta kepercayaan pengguna agar pelayanan akademik dapat berlangsung dengan lancar dan berkelanjutan.

Penelitian ini menggunakan metode ISO/IEC 27005 karena metode ini berfokus pada manajemen risiko keamanan informasi secara sistematis dan terstruktur. ISO/IEC 27005 memberikan pedoman dalam mengidentifikasi, menganalisis, mengevaluasi, serta menangani risiko yang dapat memengaruhi keamanan sistem informasi. Metode ini dinilai sesuai untuk lingkungan akademik karena mampu membantu perguruan tinggi dalam menjaga kerahasiaan data, ketersediaan sistem, dan keandalan layanan portal akademik. Dengan demikian, penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko pada Portal Akademik *New Student* UIGM menggunakan metode ISO 27005 sebagai standar manajemen risiko keamanan informasi yang diakui secara internasional [7]. Penelitian ini dilakukan karena belum adanya analisis risiko keamanan informasi secara khusus pada Portal Akademik *New Student* UIGM menggunakan metode ISO 27005. Melalui penelitian ini diharapkan dapat diketahui potensi risiko yang ada serta memberikan rekomendasi pengendalian yang tepat untuk meningkatkan keamanan dan kualitas portal akademik.

TINJAUAN PUSTAKA

Sistem Informasi

Sistem informasi adalah sebuah sistem yang termasuk dalam sebuah organisasi dan menangani transaksi sehari-hari, mendukung kegiatan operasional, administratif, dan strategis organisasi yang bisa memberikan laporan yang diperlukan kepada pihak luar [8].

Sistem Informasi adalah kombinasi teknologi informasi dan aktivitas orang yang menggunakan teknologi untuk mendukung operasi dan manajemen. Dalam arti yang sangat luas, sistem informasi merujuk

kepada interaksi antara orang, proses algoritmik, data, dan teknologi [9].

Dengan adanya SI, organisasi dapat mengolah dan menyebarkan informasi yang relevan secara efisien, baik untuk mendukung kegiatan internal maupun untuk memenuhi kebutuhan laporan kepada pihak luar. Selain itu, SI juga mencakup interaksi antara teknologi, data, dan orang, yang memungkinkan penggunaan teknologi untuk meningkatkan efektivitas dan efisiensi operasional serta manajerial dalam suatu organisasi.

Sistem Informasi Akademik

Sistem informasi akademik merupakan suatu sistem yang dirancang untuk menyediakan layanan data dan informasi yang berkaitan dengan kegiatan akademik secara terstruktur dan terintegrasi. Sistem ini dikembangkan dengan menyesuaikan kebutuhan serta proses bisnis yang berlangsung secara berkelanjutan di lingkungan pendidikan, khususnya perguruan tinggi [10]. Keberadaan sistem ini bertujuan untuk memperlancar proses akademik, meminimalkan kesalahan dalam pengolahan data, serta meningkatkan kualitas pelayanan akademik bagi mahasiswa, dosen, maupun tenaga kependidikan. Dengan demikian, sistem informasi akademik menjadi salah satu komponen penting dalam mendukung kelancaran operasional dan peningkatan mutu layanan pendidikan di perguruan tinggi.

Portal Akademik New Student UIGM

Portal akademik *New Student* Universitas Indo Global Mandiri (UIGM) merupakan salah satu bentuk penerapan teknologi informasi yang berfungsi untuk mendukung pengelolaan kegiatan akademik di perguruan tinggi. Sistem ini menjadi sarana utama bagi mahasiswa dalam mengakses berbagai layanan akademik, seperti pengisian Kartu Rencana Studi (KRS), melihat jadwal perkuliahan, memeriksa hasil studi, hingga memperoleh informasi penting lainnya yang berkaitan dengan proses pembelajaran. Selain itu, Portal akademik ini juga digunakan dalam pengelolaan administrasi, seperti pembayaran biaya pendidikan dan layanan pendukung lainnya yang terintegrasi dalam satu *platform*. Dengan adanya Portal akademik yang terstruktur, proses pengelolaan data menjadi lebih efektif, efisien, serta mampu meningkatkan kualitas pelayanan akademik di lingkungan perguruan tinggi.

Manajemen Risiko

Manajemen risiko merupakan suatu metode yang digunakan untuk mengidentifikasi, menganalisis, dan mengendalikan berbagai risiko yang dapat terjadi dalam suatu organisasi [11]. Proses ini bertujuan untuk meminimalkan dampak negatif serta mencegah gangguan yang dapat menghambat jalannya operasional organisasi. Manajemen risiko juga membantu organisasi dalam mengambil keputusan yang lebih tepat terhadap potensi ancaman yang dapat memengaruhi aktivitas kerja.

Proses manajemen risiko membantu organisasi dalam mengambil keputusan yang lebih tepat serta meningkatkan efisiensi dalam menjalankan aktivitas operasional [12]. Dengan adanya manajemen risiko, potensi terjadinya risiko yang dapat menimbulkan dampak besar dapat diminimalkan sehingga kestabilan organisasi tetap terjaga. Selain itu, manajemen risiko memungkinkan organisasi untuk mengenali ancaman sejak dini dan menyiapkan langkah penanganan yang sesuai. Hal ini penting agar setiap aktivitas dapat berjalan lebih aman, terarah, dan mendukung pencapaian tujuan organisasi secara optimal.

ISO 27005

ISO 27005 merupakan salah satu standar internasional yang memberikan panduan teknis dan metodologis untuk manajemen risiko keamanan informasi [13]. Dalam standar ini, penilaian risiko dibagi menjadi tiga tingkatan: rendah, sedang, dan tinggi, tergantung pada tingkat kompleksitas dan sumber daya organisasi. Proses manajemen risiko dalam standar ini meliputi identifikasi risiko, analisis risiko, evaluasi risiko, penanganan risiko, monitoring, komunikasi, dan konsultasi

Penelitian Terdahulu

Penelitian berjudul Analisis Manajemen Risiko Informasi Menggunakan ISO/IEC 27005:2018 (Studi Kasus: PT. XYZ) membahas penerapan manajemen risiko keamanan informasi pada aset teknologi informasi perusahaan [14]. Penelitian ini menggunakan standar ISO/IEC 27005:2018 sebagai pedoman utama dalam proses identifikasi, analisis, evaluasi, hingga pengendalian risiko keamanan informasi. Hasil penelitian menunjukkan terdapat 7 potensi ancaman utama yang memengaruhi aset utama maupun aset pendukung seperti *hardware*, *software*, dan *network*. Setiap ancaman kemudian diberikan rekomendasi pengendalian risiko berupa mitigasi, penerimaan risiko, maupun transfer risiko sesuai tingkat risikonya. Penelitian ini menunjukkan bahwa penerapan ISO/IEC 27005:2018 mampu membantu organisasi dalam menjaga keamanan informasi serta meningkatkan efektivitas pengelolaan risiko pada sistem informasi perusahaan.

Penelitian lainnya berjudul Manajemen Risiko pada Sistem Informasi Akademik Universitas XYZ Menggunakan ISO 27005:2018 membahas analisis risiko keamanan informasi pada Sistem Informasi Akademik (SIAKAD) di lingkungan perguruan tinggi [15]. Penelitian ini menggunakan standar ISO 27005:2018 untuk mengidentifikasi, menganalisis, mengevaluasi, serta menentukan perlakuan risiko yang tepat terhadap berbagai ancaman keamanan informasi. Hasil penelitian menunjukkan terdapat 4 risiko terkait data, 3 risiko terkait *software*, 6 risiko terkait *hardware*, dan 5 risiko pada kategori *people*. Dari hasil analisis ditemukan 1 risiko dengan level ekstrim dan 10 risiko dengan level tinggi, serta terdapat 6 risiko yang melebihi batas penerimaan risiko sehingga

memerlukan tindakan khusus seperti mitigasi, transfer risiko, dan kontrol akses. Penelitian ini membuktikan bahwa penerapan ISO 27005:2018 dapat membantu perguruan tinggi dalam meningkatkan keamanan sistem akademik serta mendukung pengelolaan risiko informasi secara lebih efektif dan terstruktur.

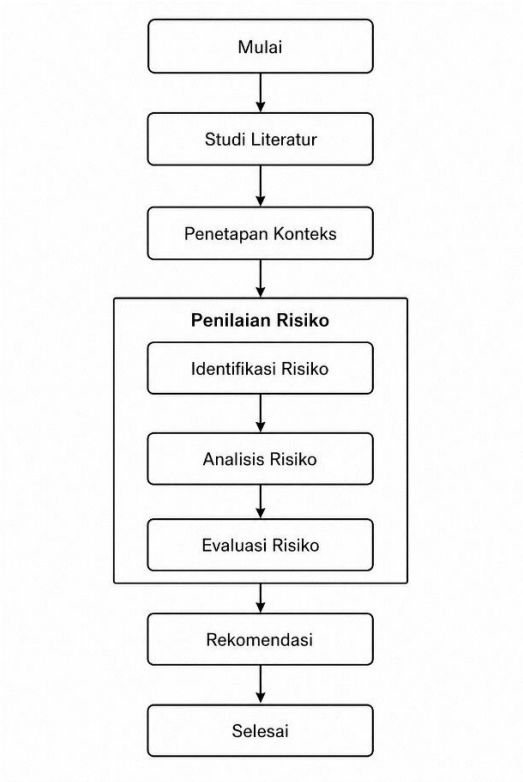
Penelitian terakhir berjudul Analisis Risiko Keamanan Informasi pada *Learning Management System* (LMS) Universitas Sebelas April Menggunakan Standar ISO 27005 membahas penerapan manajemen risiko keamanan informasi pada sistem *Learning Management System* (LMS) di Universitas Sebelas April [16]. Penelitian ini menggunakan standar ISO 27005 sebagai kerangka kerja untuk mengidentifikasi, menganalisis, mengevaluasi, serta menangani risiko keamanan informasi yang berkaitan dengan aset penting seperti data pengguna, nilai akademik, materi perkuliahan, dan infrastruktur pendukung sistem. Ancaman yang dianalisis meliputi akses tidak sah, kebocoran data, penyebaran *malware*, hingga manipulasi data akademik. Hasil penelitian diharapkan mampu menghasilkan pemetaan risiko keamanan informasi secara terstruktur serta rekomendasi strategis seperti penerapan autentikasi dua faktor (2FA), enkripsi data, pencadangan rutin, dan edukasi keamanan bagi pengguna. Penelitian ini menunjukkan bahwa penerapan ISO 27005 dapat membantu perguruan tinggi dalam memperkuat keamanan sistem pembelajaran digital dan menjaga keberlangsungan proses akademik secara aman dan efektif.

Berdasarkan beberapa penelitian terdahulu, analisis manajemen risiko keamanan informasi menggunakan standar ISO 27005:2018 telah banyak diterapkan pada perusahaan, Sistem Informasi Akademik (SIAKAD), serta *Learning Management System* (LMS). Pada penelitian ini, penulis memilih Portal Akademik *New Student* di Universitas Indo Global Mandiri (UIGM) sebagai objek penelitian. Kebaruan penelitian ini terletak pada fokus pada Manajemen risiko Sistem informasi Portal Akademik *New Student* UIGM dengan menggunakan Metode ISO 27005, sehingga diharapkan dapat memberikan rekomendasi pengendalian risiko yang lebih sesuai untuk meningkatkan keamanan, keandalan, dan kualitas layanan sistem akademik kampus.

METODOLOGI PENELITIAN

Tahapan Penelitian

Tahapan penelitian menjelaskan langkah-langkah yang dilakukan dalam proses penelitian secara sistematis dan terstruktur. Tahapan ini disusun untuk memudahkan pelaksanaan penelitian agar sesuai dengan tujuan yang ingin dicapai. Dalam penelitian ini, tahapan dimulai dari studi literatur, penetapan konteks, penilaian risiko yang meliputi identifikasi risiko, analisis risiko, dan evaluasi risiko, hingga penyusunan rekomendasi. Setiap tahap memiliki peran penting dalam mendukung proses analisis manajemen risiko keamanan informasi pada Portal Akademik *New Student* Universitas Indo Global Mandiri (UIGM) menggunakan metode ISO 27005. Berikut adalah tahapan penelitian yang dilakukan dalam menganalisis manajemen risiko keamanan informasi pada Portal Akademik *New Student* Universitas Indo Global Mandiri (UIGM) menggunakan metode ISO 27005 [7].



Gambar 1. Tahapan Penelitian
Sumber : Olah Data

Studi Literatur

Tahap ini dilakukan dengan mengumpulkan berbagai referensi yang relevan seperti jurnal, buku, penelitian terdahulu, dan sumber ilmiah lainnya yang berkaitan dengan manajemen risiko keamanan informasi, sistem informasi akademik, serta penerapan metode ISO 27005. Tujuannya adalah untuk memperoleh landasan teori yang kuat sebagai dasar penelitian.

Penetapan Konteks

Tahap penetapan konteks dilakukan untuk menentukan ruang lingkup penelitian agar proses analisis risiko lebih terarah dan sesuai dengan kondisi sistem yang diteliti. Pada tahap ini, peneliti menetapkan objek penelitian yaitu Portal Akademik *New Student* Universitas Indo Global Mandiri (UIGM) sebagai sistem yang digunakan mahasiswa untuk mengakses berbagai layanan akademik. Selain itu, ditentukan juga aset-aset penting yang terdapat dalam sistem, seperti data mahasiswa, informasi akademik, data pembayaran, serta infrastruktur pendukung sistem. Penetapan konteks juga mencakup identifikasi pihak-pihak yang terlibat,

seperti mahasiswa, admin akademik, dan pihak pengelola sistem, sehingga proses analisis risiko dapat dilakukan secara lebih jelas dan terfokus.

Penilaian Risiko

Tahap penilaian risiko merupakan proses utama dalam penelitian yang dilakukan untuk mengetahui tingkat risiko pada Portal Akademik *New Student* UIGM. Pada tahap ini, penilaian risiko mencakup tiga bagian, yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko. Identifikasi risiko dilakukan dengan menemukan berbagai potensi ancaman, kerentanan, serta sumber risiko yang dapat memengaruhi keamanan dan kinerja sistem, seperti gangguan sistem, error saat penggunaan, kebocoran data, akses tidak sah, serangan siber, hingga kegagalan *server* atau jaringan. Setelah risiko diidentifikasi, dilakukan analisis risiko untuk menilai tingkat kemungkinan terjadinya risiko dan besarnya dampak yang ditimbulkan terhadap sistem akademik. Selanjutnya, tahap evaluasi risiko dilakukan untuk menentukan prioritas penanganan berdasarkan tingkat risiko yang telah diperoleh. Risiko dengan tingkat tinggi akan menjadi fokus utama untuk segera dikendalikan, sedangkan risiko dengan tingkat rendah dapat dipantau secara berkala. Tahap ini menjadi dasar dalam penyusunan strategi pengendalian risiko yang tepat untuk meningkatkan keamanan dan keandalan sistem.

Rekomendasi

Tahap rekomendasi merupakan tahap akhir dalam penelitian yang bertujuan untuk memberikan usulan pengendalian dan perbaikan terhadap risiko yang telah dianalisis pada Portal Akademik *New Student* UIGM. Rekomendasi disusun berdasarkan hasil penilaian risiko dengan fokus pada risiko yang memiliki tingkat tinggi dan berpotensi mengganggu keamanan serta operasional sistem. Bentuk rekomendasi dapat berupa peningkatan keamanan sistem, perbaikan performa *server*, penguatan kontrol akses pengguna, pencadangan data secara berkala, peningkatan *monitoring* sistem, serta penyediaan dukungan teknis yang lebih optimal. Tahap ini diharapkan dapat membantu pihak kampus dalam meminimalkan risiko, menjaga keberlangsungan layanan akademik, serta meningkatkan keandalan dan kualitas Portal Akademik *New Student* UIGM.

Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian deskriptif dengan pendekatan kualitatif. Penelitian deskriptif bertujuan untuk menggambarkan kondisi nyata yang terjadi pada Portal Akademik *New Student* Universitas Indo Global Mandiri (UIGM), khususnya yang berkaitan dengan risiko keamanan informasi dan operasional sistem. Pendekatan kualitatif digunakan untuk memahami berbagai potensi risiko, ancaman, serta kerentanan yang dapat memengaruhi keamanan dan keandalan sistem melalui observasi serta penyebaran kuesioner kepada pengguna. Penelitian ini juga didukung dengan penerapan metode ISO 27005 sebagai kerangka kerja dalam proses identifikasi, analisis, evaluasi, dan penyusunan rekomendasi pengendalian risiko. Dengan demikian, penelitian ini diharapkan dapat memberikan gambaran yang jelas mengenai kondisi manajemen risiko pada portal akademik serta solusi yang tepat untuk meningkatkan kualitas sistem informasi akademik.

HASIL DAN PEMBAHASAN

Studi Literatur

Dari hasil studi literatur diketahui bahwa Portal Akademik *New Student* UIGM memiliki peran penting dalam mendukung kegiatan akademik mahasiswa, khususnya dalam proses pengisian KRS, pengecekan jadwal kuliah, hasil studi, hingga pembayaran administrasi. Karena sistem ini digunakan secara rutin dan menyimpan data penting, maka potensi risiko seperti gangguan sistem, *error*, kebocoran data, dan akses tidak sah perlu menjadi perhatian utama.

Selain itu, penelitian terdahulu menunjukkan bahwa metode ISO 27005 banyak digunakan dalam analisis manajemen risiko karena memiliki tahapan yang jelas dan terstruktur, mulai dari identifikasi risiko hingga rekomendasi penanganan. Oleh karena itu, metode ini dipilih karena dianggap sesuai untuk digunakan dalam menganalisis risiko pada Portal Akademik *New Student* UIGM. Hasil dari tahap ini menjadi dasar untuk melanjutkan penelitian pada tahap penetapan konteks dan penilaian risiko.

Penetapan Konteks

Pada penelitian ini, objek yang dianalisis adalah Portal Akademik *New Student* Universitas Indo Global Mandiri (UIGM), yaitu sistem yang digunakan mahasiswa untuk mengakses berbagai layanan akademik seperti pengisian KRS, melihat jadwal perkuliahan, pengecekan hasil studi, serta pembayaran administrasi.

Pada tahap ini, peneliti juga mengidentifikasi aset-aset penting yang terdapat dalam sistem, seperti data pribadi mahasiswa, data akademik, data pembayaran, serta *server* dan jaringan yang mendukung operasional portal akademik. Aset-aset tersebut memiliki nilai penting karena berhubungan langsung dengan keberlangsungan layanan akademik dan keamanan informasi pengguna.

Selain itu, pihak-pihak yang terlibat dalam penggunaan sistem juga ditentukan, seperti mahasiswa sebagai pengguna utama, admin akademik sebagai pengelola data, serta pihak teknis atau administrator sistem yang bertanggung jawab terhadap pemeliharaan portal akademik. Penetapan konteks ini bertujuan agar proses identifikasi dan penilaian risiko dapat dilakukan secara lebih fokus, sehingga hasil analisis yang diperoleh lebih relevan dan sesuai dengan kebutuhan sistem.

Penilaian Risiko

Pada tahap ini, penilaian risiko dilakukan melalui tiga proses, yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko. Tujuannya adalah untuk mengetahui potensi ancaman yang dapat mengganggu keamanan informasi serta operasional sistem akademik.

Identifikasi Risiko

Identifikasi risiko dilakukan berdasarkan hasil observasi, penyebaran kuesioner kepada responden, serta studi literatur yang berkaitan dengan manajemen risiko keamanan informasi. Kuesioner disebarkan dan mendapatkan 70 responden mahasiswa UIGM dengan 15 pernyataan dengan pola jawaban skala Likert 1–5.

Berdasarkan hasil kuesioner, pola jawaban menunjukkan bahwa nilai yang paling sering muncul berada pada rentang 3 hingga 4, yang mengindikasikan bahwa sebagian besar responden berada pada posisi netral hingga setuju terhadap kualitas sistem. Beberapa aspek seperti keamanan proses login, penyimpanan data pribadi, serta perlindungan terhadap risiko kehilangan data memperoleh penilaian yang relatif lebih tinggi, dengan skor dominan pada nilai 4.

Meskipun demikian, masih terdapat beberapa aspek yang mendapatkan penilaian lebih rendah, terutama pada stabilitas sistem, kecepatan respons, serta gangguan saat penggunaan portal. Hal ini terlihat dari adanya skor 2 pada beberapa pernyataan yang berkaitan dengan error sistem dan kendala penggunaan. Selain itu, kemampuan sistem dalam menangani jumlah pengguna yang besar secara bersamaan juga masih dinilai belum optimal oleh sebagian responden.

Berdasarkan temuan tersebut, dapat diidentifikasi beberapa risiko yang berpotensi terjadi, seperti sistem yang sering mengalami gangguan saat banyak pengguna mengakses portal, *error* pada saat pengisian KRS, lambatnya respons sistem, kesalahan input data akademik, akses oleh pihak yang tidak berwenang, kebocoran data mahasiswa, gangguan jaringan internet, serta risiko kehilangan data akibat tidak adanya pencadangan data secara rutin. Risiko-risiko tersebut berpotensi mengganggu kelancaran proses akademik serta menurunkan kepercayaan pengguna terhadap sistem informasi akademik yang digunakan.

Analisis Risiko

Penilaian *likelihood* dilakukan berdasarkan seberapa sering risiko tersebut berpotensi terjadi, sedangkan *impact* dinilai berdasarkan seberapa besar pengaruh risiko tersebut terhadap operasional sistem akademik. Risiko seperti gangguan sistem saat jam sibuk, *error* pada pengisian KRS, serta kebocoran data mahasiswa memiliki tingkat kemungkinan dan dampak yang cukup tinggi karena dapat menghambat proses akademik dan mengganggu keamanan informasi pengguna.

Sementara itu, risiko seperti kesalahan input data, gangguan jaringan internet, dan keterlambatan respons sistem berada pada tingkat sedang karena masih dapat dikendalikan namun tetap memerlukan perhatian. Hasil analisis ini digunakan untuk menentukan klasifikasi risiko ke dalam kategori rendah, sedang, atau tinggi sesuai dengan pendekatan ISO 27005, sehingga memudahkan proses evaluasi risiko pada tahap berikutnya. Tabel 1 dibawah ini merupakan hasil Analisis Risiko Berdasarkan *Likelihood* dan *Impact* pada Portal Akademik *New Student* UIGM.

Tabel 1. Analisis Risiko Berdasarkan *Likelihood* dan Impact

No	Risiko	*Likelihood*	*Impact*	Tingkat Risiko
1	Sistem sering mengalami gangguan	Tinggi	Tinggi	Tinggi
2	*Error* saat pengisian KRS	Tinggi	Tinggi	Tinggi
3	Kebocoran data mahasiswa	Sedang	Tinggi	Tinggi
4	Kesalahan input data akademik	Sedang	Sedang	Sedang
5	Lambatnya respons sistem	Sedang	Sedang	Sedang
6	Gangguan jaringan internet	Sedang	Sedang	Sedang
7	Kehilangan data penting	Rendah	Tinggi	Sedang

Evaluasi Risiko

Risiko dengan kategori tinggi menjadi prioritas utama karena memiliki kemungkinan terjadinya yang besar serta dampak yang signifikan terhadap operasional Portal Akademik *New Student* UIGM. Risiko seperti sistem yang sering mengalami gangguan, error saat pengisian KRS, dan kebocoran data mahasiswa memerlukan tindakan pengendalian yang lebih cepat karena dapat menghambat proses akademik dan menurunkan kepercayaan pengguna terhadap sistem.

Sementara itu, risiko dengan kategori sedang seperti kesalahan *input* data, lambatnya respons sistem, gangguan jaringan internet, dan kehilangan data penting tetap perlu diperhatikan melalui monitoring rutin dan perbaikan bertahap. Evaluasi risiko ini menjadi dasar dalam penyusunan rekomendasi pengendalian agar penanganan yang dilakukan lebih tepat sasaran dan sesuai dengan tingkat urgensi masing-masing risiko. Tabel 2 dibawah ini merupakan hasil Evaluasi Risiko dan Prioritas Penanganan pada Portal Akademik *New Student* UIGM.

Tabel 2. Evaluasi Risiko dan Prioritas Penanganan

No	Risiko	Tingkat Risiko	Prioritas Penanganan
1	Sistem sering mengalami gangguan	Tinggi	Sangat Prioritas
2	Error saat pengisian KRS	Tinggi	Sangat Prioritas
3	Kebocoran data mahasiswa	Tinggi	Sangat Prioritas
4	Kesalahan input data akademik	Sedang	Prioritas Menengah
5	Lambatnya respons sistem	Sedang	Prioritas Menengah
6	Gangguan jaringan internet	Sedang	Prioritas Menengah
7	Kehilangan data penting	Sedang	Prioritas Menengah

Rekomendasi

Untuk mengatasi risiko sistem yang sering mengalami gangguan dan error saat pengisian KRS, diperlukan peningkatan kapasitas *server* serta pemeliharaan sistem secara berkala agar performa portal tetap stabil, terutama pada saat banyak pengguna mengakses secara bersamaan. Selain itu, monitoring sistem secara *real-time* juga perlu dilakukan untuk mendeteksi gangguan lebih cepat.

Pada risiko kebocoran data mahasiswa, rekomendasi yang dapat dilakukan adalah memperkuat kontrol akses pengguna, menerapkan autentikasi yang lebih aman, serta melakukan *backup* data secara rutin untuk menjaga kerahasiaan dan ketersediaan informasi. Edukasi kepada pengguna dan admin mengenai pentingnya keamanan data juga perlu ditingkatkan untuk mengurangi risiko penyalahgunaan akses.

Sementara itu, untuk risiko dengan kategori sedang seperti kesalahan input data, lambatnya respons sistem, dan gangguan jaringan internet, diperlukan peningkatan kualitas infrastruktur jaringan, validasi data yang lebih baik, serta dukungan teknis yang responsif. Dengan adanya rekomendasi ini, diharapkan Portal Akademik *New Student* UIGM dapat menjadi lebih aman, andal, dan mampu memberikan pelayanan akademik yang lebih optimal bagi seluruh pengguna.

KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian mengenai analisis manajemen risiko keamanan informasi pada Portal Akademik *New Student* Universitas Indo Global Mandiri (UIGM) menggunakan metode ISO 27005, dapat disimpulkan bahwa portal akademik memiliki peran penting dalam mendukung proses akademik mahasiswa, mulai dari pengisian KRS, pengecekan jadwal kuliah, hasil studi, hingga pembayaran administrasi. Namun, dalam penerapannya masih terdapat beberapa risiko yang dapat memengaruhi keamanan dan keandalan sistem.

Hasil identifikasi risiko menunjukkan adanya beberapa risiko utama seperti sistem yang sering mengalami gangguan, *error* saat pengisian KRS, kebocoran data mahasiswa, kesalahan input data akademik, lambatnya respons sistem, gangguan jaringan internet, serta kehilangan data penting. Berdasarkan analisis risiko, terdapat tiga risiko dengan tingkat tinggi yaitu sistem sering mengalami gangguan, *error* saat pengisian KRS, dan kebocoran data mahasiswa. Sementara itu, risiko lainnya berada pada tingkat sedang dan tetap memerlukan perhatian melalui monitoring dan pengendalian secara berkala.

Melalui tahap evaluasi risiko, diketahui bahwa risiko dengan kategori tinggi menjadi prioritas utama untuk segera ditangani karena dapat menghambat aktivitas akademik dan menurunkan kepercayaan pengguna terhadap sistem. Oleh karena itu, rekomendasi yang diberikan meliputi peningkatan kapasitas *server*, penguatan kontrol akses, backup data secara rutin, peningkatan *monitoring* sistem, serta perbaikan infrastruktur jaringan. Dengan penerapan rekomendasi tersebut, diharapkan Portal Akademik *New Student* UIGM dapat menjadi lebih aman, andal, dan mampu memberikan pelayanan akademik yang lebih optimal.

Berdasarkan hasil penelitian yang telah dilakukan, penulis memberikan beberapa saran yang dapat digunakan sebagai bahan pertimbangan dalam meningkatkan keamanan dan keandalan Portal Akademik *New Student* UIGM. Pihak kampus diharapkan dapat melakukan evaluasi sistem secara berkala, terutama pada aspek performa *server*, stabilitas sistem, dan keamanan data pengguna agar risiko yang telah diidentifikasi dapat diminimalkan.

Selain itu, diperlukan peningkatan kontrol akses dan perlindungan data untuk mencegah terjadinya kebocoran informasi penting mahasiswa. Proses *backup* data secara rutin juga perlu diterapkan agar risiko kehilangan data dapat dihindari. Dukungan teknis yang responsif serta monitoring sistem secara *real-time* juga sangat penting untuk mempercepat penanganan jika terjadi gangguan pada portal akademik.

Untuk penelitian selanjutnya, disarankan agar dilakukan pengembangan dengan menggunakan metode manajemen risiko lain sebagai perbandingan, seperti OCTAVE atau NIST, sehingga dapat memberikan hasil analisis yang lebih luas dan mendalam mengenai keamanan sistem informasi akademik.

DAFTAR PUSTAKA

[1] N. Ariati, A. Kamandanu, P. Maharani, A. W. Pratama, and D. P. Febriansyah, "Analisis Perencanaan Strategis Sistem Informasi Menggunakan Metode Ward and Peppard," *RIGGS J. Artif. Intell. Digit. Bus.*, vol. 4, no. 4 SE-Articles, pp. 10433–10440, Jan. 2026, doi: 10.31004/riggs.v4i4.5141.

[2] A. A. Zulfa, T. Ibrahim, and O. Arifudin, "PERAN SISTEM INFORMASI AKADEMIK BERBASIS WEB DALAM UPAYA MENINGKATKAN EFEKTIVITAS DAN EFISIENSI

PENGELOLAAN AKADEMIK DI PERGURUAN TINGGI," *J. Tahsinia*, vol. 6, no. 1, pp. 115–134, 2025.

[3] Winda Widiastuti, Rohayanah, and Ine Rahayu Purnamaningsih, "MANAJEMEN MUTU PENDIDIKAN BERBASIS DIGITAL: PENGARUH IMPLEMENTASI SISTEM INFORMASI PENDIDIKAN TERHADAP KINERJA AKADEMIK DI PERGURAN TINGGI," *J. Dev.*, vol. 13, no. 1 SE-Management, pp. 161–173, Jun. 2025, doi: 10.53978/jd.v13i1.572.

[4] K. Nadiya, N. C. Nisa, S. A. N. Aini, and A. U. P. S. Jandi, "ANALISIS MANAJEMEN RISIKO PADA SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK OCTAVE ALLEGRO," *JORAPI J. Res. Publ. Innov.*, vol. 2, no. 2, pp. 1479–1491, 2024.

[5] R. S. Ayu, M. M. Rivai, N. Al Mubarak, and D. Pratama, "KEAMANAN INFRASTRUKTUR TEKNOLOGI INFORMASI: ANALISIS ANCAMAN SIBER DAN PENDEKATAN MITIGASI," *J. Pendidik. Sos. dan Hum.*, vol. 4, no. 2, pp. 2598–2609, 2025.

[6] S. Paramita, "ANALISIS MANAJEMEN TIK TERHADAP KEAMANAN INFORMASI DAN MANAJEMEN RISIKO PERPUSTAKAAN," *JIMSI J. Teknol. dan Manaj. Sist. Ind.*, vol. 2, no. 1, pp. 58–64, 2023, doi: 10.56071/jtmsi.v2i1.469.

[7] A. N. Fanani, B. T. Hanggara, and A. R. Perdanakusuma, "Manajemen Risiko Keamanan Informasi Menggunakan ISO / IEC 27005 Studi Kasus Pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 6, pp. 1–9, 2025.

[8] Lalu. M. Nisa. J. Urnika. W. Farid. Sepriano. D. Aulia. S. Ahmad. Kharisma, *Analisis Dan Perancangan Sistem Berbasis Studi Kasus*, no. May. 2023. [Online]. Available: https://books.google.com/books?hl=en%5C&lr=%5C&id=DCnBEAAAQBAJ%5C&oi=fnd%5C&pg=PA27%5C&dq=privasi+personal+health+record+dalam+tindakan+pelanggaran+ham%5C&ots=KzuNcAcCJY%5C&sig=l4PU8SDbm8k1Ju9TpbreaS11-Ug

[9] F. Syahputra and M. A. Saptari, "Aplikasi Sistem Informasi Pemesanan Iklan Berbasis Web," *Sisfo J. Ilm. Sist. Inf.*, vol. 7, no. 1, p. 46, 2023, doi: 10.29103/sisfo.v7i1.12105.

[10] S. N. Oktaviana, V. Apriliani, W. N. Novita, S. Mulyeni, and H. Herlina, "Implementasi Sistem Informasi Akademik Dalam Meningkatkan Mutu Pelayanan Kampus," *J. Soshum Insentif*, vol. 7, no. 1, pp. 53–62, 2024.

[11] L. E. Hutagalung, "ANALISA MANAJEMEN RISIKO SISTEM INFORMASI MANAJEMEN RUMAH SAKIT (SIMRS) PADA RUMAH SAKIT XYZ MENGGUNAKAN ISO 31000," *J. TelKa*, vol. 12, no. 1, pp. 23–33, 2022.

[12] R. Bisma, "Manajemen Risiko Aset Teknologi Informasi : Studi kasus Implementasi Manajemen Risiko SPBE Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan," *JIEET J. Inf. Eng. Educ. Technol.*, vol. 06, no. 2, pp. 73–79, 2022.

[13] N. A. Chandra and M. Yusuf, "Penilaian Resiko Keamanan Aplikasi Web Menggunakan Standar ISO/IEC 27005 : 20022 Pada Layanan Organisasi," *J. Comput. Sci. Inf. Technol. (CoSciTech)*, vol. 6, no. 2, pp. 206–213, 2025.

[14] M. L. B. Hikam, F. Dewi, and D. Praditya, "Analisis Manajemen Risiko Informasi Menggunakan ISO/IEC 27005:2018 (Studi Kasus: PT.XYZ)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 2, pp. 728–734, 2024.

[15] Z. V. Leasa and G. F. Prassida, "Manajemen Risiko pada Sistem Informasi Akademik Universitas XYZ Menggunakan ISO 27005 : 2018," *JTeksis (Jurnal Teknol. dan Sist. Inf. Bisnis*, vol. 6, no. 4, pp. 649–656, 2024.

[16] I. I. Aryani, "Analisis Risiko Keamanan Informasi pada Learning Management System (LMS) Universitas Sebelas April Menggunakan Standar ISO 27005," *Infoman's J. Ilmu-ilmu Inform. dan Manaj.*, vol. 19, no. 1, pp. 1–5, 2025.