NIVEDITA
JOURNAL INFORMATICS
e-ISSN : xxx-xxx
p-ISSN : xxx-xxx

Vol. 01, No. 1, Desember 2024

ANALISIS DAMPAK RISIKO IT PADA WEBSITE SISTEM INFORMASI PELAYANAN ADMINISTRASI SURAT MENYURAT (SIASY) MENGGUNAKAN METODE FMEA

Cindy Kirana Zarry[1], Muthia Tshamaroh[2], Suci Agesti[3], Megawati[4]

[1234]Sistem Informasi,Sains dan Teknologi,Universitas Islam Negeri Sultan Syarif Kasim Riau

email: [1]12150322263@students.uin-suska.ac.id , [2]12150311139@students.uin-suska.ac.id , [3]12150323229@students.uin-suska.ac.id, [4]megawati@uin-suska.ac.id

Abstract

The Administrative Correspondence Service Information System (SIASY) in higher education institutions faces various challenges and IT risks that can disrupt the efficiency of administrative services. Issues such as limited access for management, data inaccuracies, and synchronization problems with the financial system are key focuses that need to be analyzed to enhance system reliability. This study aims to explore the application of the Failure Mode and Effects Analysis (FMEA) method in identifying and managing the risks present in SIASY. It is expected to provide recommendations for system administrators to improve the quality and reliability of administrative services. The FMEA method also serves to identify weaknesses in the system, evaluate associated risks, and provide solutions to mitigate existing issues. The data used in this study includes information about the administrative processes conducted through SIASY, as well as results from interviews and surveys with system users (students, lecturers, and staff) to gain insights into their challenges and needs. The research findings indicate that the application of FMEA can assist in identifying and managing the IT risks present in SIASY. By addressing issues such as limited access, data inaccuracies, and system synchronization, it is expected that efficiency and user satisfaction in the administrative processes at higher education institutions can be improved. This study provides significant contributions for system administrators in their efforts to enhance the reliability and quality of administrative services.

Keywords: *Information System, Effect Of IT Risks, SIASY, FMEA.*

Abstrak

Sistem Informasi Pelayanan Administrasi Surat Menyurat (SIASY) di perguruan tinggi menghadapi berbagai tantangan dan risiko IT yang dapat mengganggu efisiensi layanan administrasi. Isu-isu seperti akses terbatas bagi pimpinan, ketidakakuratan data, dan masalah sinkronisasi dengan sistem keuangan menjadi fokus utama yang perlu dianalisis untuk meningkatkan keandalan sistem. Penelitian ini bertujuan untuk mengeksplorasi penerapan metode *Failure Mode and Effects Analysis* (FMEA) dalam mengidentifikasi dan mengelola risiko yang ada pada SIASY. Dengan demikian, diharapkan dapat memberikan rekomendasi bagi pengelola sistem untuk meningkatkan kualitas dan keandalan layanan administrasi. Metode FMEA juga berguna untuk mengidentifikasi titik-titik lemah dalam sistem, mengevaluasi risiko yang terkait, dan memberikan solusi untuk memitigasi masalah yang ada. Data yang digunakan dalam riset ini meliput informasi tentang proses administrasi yang dilakukan melalui SIASY, serta hasil wawancara dan survei dengan pengguna sistem (mahasiswa, dosen, dan pegawai) untuk mendapatkan wawasan mengenai tantangan dan kebutuhan mereka. Hasil penelitian menunjukkan bahwa penerapan FMEA dapat membantu dalam mengidentifikasi dan mengelola risiko TI yang ada pada SIASY. Dengan mengatasi masalah seperti akses terbatas, ketidakakuratan data, dan sinkronisasi sistem, diharapkan efisiensi dan kepuasan pengguna dalam proses administrasi di perguruan tinggi dapat meningkat. Penelitian ini memberikan kontribusi penting bagi pengelola sistem dalam upaya meningkatkan keandalan dan kualitas layanan administrasi.

Kata kunci: Sistem Informasi, Dampak Risiko TI, SIASY, FMEA.

Diajukan: 11 Desember 2024; Diterima: 10 Januari 2025;

PENDAHULUAN

Di era digital saat ini, penggunaan sistem informasi dalam berbagai aspek kehidupan, termasuk dalam layanan administrasi pendidikan, menjadi semakin penting. Salah satu sistem yang memiliki peran penting adalah Sistem Informasi Pelayanan Administrasi Surat Menyurat (SIASY), yang dirancang untuk mempermudah mahasiswa, dosen, dan pegawai dalam mengelola proses administrasi surat menyurat. Namun, meskipun sistem ini telah memberikan kemudahan, masih terdapat sejumlah tantangan yang perlu diatasi untuk meningkatkan efektivitas dan kehandalannya[1].

Sistem SIASY yang ada saat ini masih memiliki banyak kekurangan dan memerlukan perbaikan untuk mencapai tingkat yang lebih optimal. Beberapa masalah yang dihadapi termasuk akses yang terbatas bagi pimpinan dan kebutuhan untuk melapor kepada PTIPD setiap kali ada penambahan data. Hal ini menunjukkan adanya kesenjangan dalam manajemen data yang dapat menghambat proses administrasi dan pengambilan keputusan yang tepat waktu. Ketidaksesuaian ini tidak hanya memperlambat proses pengambilan keputusan strategis karena informasi penting tidak tersedia secara langsung, tetapi juga menunjukkan kurangnya otonomi operasional dalam sistem, sehingga mengurangi efisiensi dan kelincahan organisasi dalam merespons kebutuhan. Keberadaan sistem yang tidak sinkron dengan sistem keuangan, khususnya dalam hal pembayaran UKT, juga menjadi perhatian serius, karena dapat menyebabkan ketidakakuratan dalam pengelolaan data keuangan mahasiswa[2].

Permasalahan yang dihadapi oleh sistem SIASY menunjukkan perlunya dilakukan analisis risiko. Risiko Keputusan yang terkait Keterlambatan dalam pengambilan keputusan akibat kurangnya akses informasi yang tepat waktu. Risiko Finansial yang terkait Ketidakakuratan data keuangan mahasiswa yang dapat mengakibatkan kesalahan dalam pengelolaan pembayaran UKT. Lalu, Risiko Operasional yang terkait Efisiensi organisasi terhambat karena proses administrasi yang lambat dan kurangnya otonomi yang membuat permasalahan ini perlu dilakukan analisis risiko lebih lanjut.

Salah satu kelompok yang paling terpengaruh oleh masalah ini adalah mahasiswa. Mereka sering kali mengalami kesulitan dalam mengakses informasi penting terkait administrasi, termasuk nama program studi yang tidak bisa diakses tanpa input manual. Selain itu, data mahasiswa baru tidak terinput dengan baik pada awal semester, yang dapat mengakibatkan keterlambatan dalam proses akademik. Hal ini menimbulkan pertanyaan tentang bagaimana analisis dampak risiko IT dapat diterapkan untuk meningkatkan keandalan dan kinerja sistem SIASY[3].

Analisis risiko IT merupakan aspek yang krusial dalam pengembangan dan pengelolaan sistem informasi. Dalam konteks SIASY, penting untuk menerapkan metode yang tepat untuk mengidentifikasi, menganalisis, dan memitigasi risiko yang ada. Salah satu metode yang banyak digunakan adalah Failure Mode and Effects Analysis (FMEA), yang dapat membantu dalam mengidentifikasi potensi kegagalan dalam sistem dan dampaknya terhadap operasional. FMEA berfokus pada identifikasi mode kegagalan potensial dalam suatu sistem. Dalam kasus SIASY, berbagai masalah seperti akses terbatas, ketidaksesuaian dengan sistem keuangan, dan proses pelaporan yang tidak efisien semuanya dapat dianggap sebagai mode kegagalan. Metode ini memungkinkan tim untuk mengidentifikasi dan menganalisis setiap mode kegagalan secara sistematis. FMEA tidak hanya mengidentifikasi mode kegagalan tetapi juga mengevaluasi dampak dari setiap kegagalan serta kemungkinan terjadinya. Dengan menilai dampak keterlambatan dalam pengambilan keputusan dan risiko ketidakakuratan data keuangan, FMEA memberikan gambaran jelas tentang risiko yang dihadapi dan prioritas tindakan yang diperlukan. FMEA memungkinkan identifikasi mendalam terhadap titik-titik lemah dalam sistem, seperti akses terbatas bagi pimpinan dan ketidaksinkronan dengan sistem keuangan. Dengan metode ini, setiap potensi kegagalan dapat diuraikan berdasarkan dampak, kemungkinan terjadinya, dan kemampuan deteksinya. Dengan menerapkan FMEA, tim pengelola SIASY dapat merumuskan strategi yang lebih efektif untuk mengurangi risiko dan meningkatkan keandalan sistem[4].

Dan diketahui bahwa sistem SIASY belum pernah mengalami peretasan, namun pernah mengalami error beberapa hari. Kejadian ini menunjukkan bahwa meskipun sistem masih aman dari serangan eksternal, masih terdapat risiko internal yang perlu dikelola dengan baik. Maintenance yang dilakukan langsung oleh PTIPD juga perlu dievaluasi untuk memastikan bahwa semua aspek sistem berfungsi dengan baik dan dapat diakses oleh seluruh pengguna secara efektif[3].

Di sisi lain, belum adanya standar atau kebijakan khusus dari fakultas terkait analisis dampak risiko IT menunjukkan bahwa masih ada ruang untuk perbaikan. Kebijakan yang jelas dan terstruktur sangat penting untuk menghadapi berbagai tantangan yang muncul dalam pengelolaan sistem informasi. Dengan adanya kebijakan yang baik, diharapkan proses analisis dampak risiko dapat dilakukan secara lebih sistematis dan terencana[5].

Melihat kebutuhan akan analisis dampak risiko yang lebih baik, penelitian ini memiliki tujuan untuk mengeksplorasi penerapan metode FMEA dalam mengidentifikasi dan mengelola risiko yang ada pada

SIASY. Dengan pendekatan ini, diharapkan akan mendapatkan solusi yang efektif untuk mengatasi permasalahan yang ada dan meningkatkan kualitas layanan administrasi yang diberikan kepada mahasiswa dan staf[4].

Penelitian ini sangat relevan, mengingat pentingnya sistem informasi dalam mendukung kegiatan akademik dan administrasi di perguruan tinggi. Dengan sistem yang handal dan aman, diharapkan dapat meningkatkan kepuasan pengguna dan efisiensi dalam proses administrasi. Hal ini pada akhirnya akan berkontribusi pada peningkatan kualitas pendidikan secara keseluruhan[6].

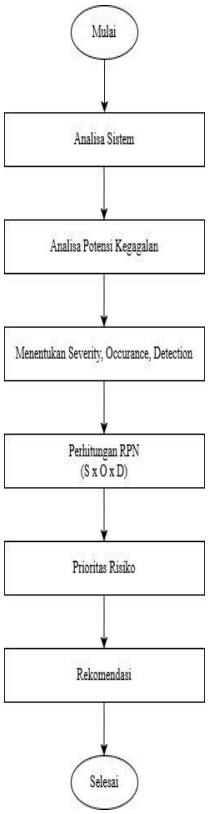
Sebagai langkah awal dalam penelitian ini, penting untuk melakukan analisis mendalam terhadap kondisi saat ini dari sistem SIASY, serta mengidentifikasi potensi risiko yang ada. Dengan ini, peneliti berharap akan dapat memberikan rekomendasi yang konkret bagi pihak pengelola untuk meningkatkan manajemen risiko IT pada sistem informasi pelayanan administrasi[3].

METODE

Penelitian ini menggunakan pendekatan deskriptif dengan metode analisis risiko berbasis Failure Mode and Effects Analysis (FMEA). Pendekatan ini bertujuan untuk mengidentifikasi, menganalisis, dan memberikan solusi atas potensi kegagalan dalam Sistem Informasi Pelayanan Administrasi Surat Menyurat (SIASY). Penelitian ini bersifat kuantitatif dan kualitatif, di mana data yang digunakan mencakup data primer dan sekunder.

Data primer diperoleh melalui wawancara langsung dengan admin SIASY dan responden lainnya yang relevan, seperti kepala sub bagian koordinator, dosen, dan mahasiswa. Selain itu, data juga dikumpulkan melalui distribusi kuesioner kepada pengguna sistem untuk mendapatkan informasi yang lebih terukur dan terstruktur. Data sekunder berupa dokumen internal dan catatan sistem yang memberikan gambaran tentang proses dan permasalahan operasional SIASY.

Penelitian ini menggunakan teknik purposive sampling, di mana responden dipilih berdasarkan peran dan relevansi mereka terhadap sistem SIASY. Subjek penelitian mencakup admin sistem yang bertanggung jawab langsung atas pengelolaan, kepala bagian yang memiliki otoritas pengambilan keputusan, serta dosen dan mahasiswa sebagai pengguna akhir. Pemilihan sampel ini bertujuan untuk mendapatkan perspektif yang komprehensif mengenai tantangan dan risiko yang dihadapi oleh sistem.



Gambar 1. Metodologi Penelitian

1. Analisa Sistem

Analisa sistem adalah tahapan yang bertujuan untuk mengidentifikasi dan memahami komponen-komponen dari sistem yang sedang diteliti, termasuk interaksi antar komponen tersebut. Proses ini mencakup pengumpulan data, pemodelan, dan evaluasi kebutuhan pengguna untuk memastikan bahwa sistem dapat memenuhi tujuan yang ditetapkan[7]. (Lihat **Gambar 1**, tahap pertama).

2. Analisa Potensi Kegagalan

Analisa potensi kegagalan merupakan metode yang dapat mengidentifikasi kemungkinan hal negatif atau kegagalan dalam sistem dan dampaknya terhadap kinerja. Metode ini sering kali melibatkan teknik Failure Mode and Effects Analysis (FMEA), yang membantu peneliti untuk memahami titik lemah dalam sistem[8]. (Lihat **Gambar 1**, tahap kedua).

3. Menentukan Severity, Occurrence, Detection

Dalam analisa potensi kegagalan, ada tiga parameter utama yang perlu ditentukan yaitu: Severity (S), yang menilai dampak kegagalan; Occurrence (O), yang menghitung frekuensi terjadinya kegagalan; dan Detection (D), yang menilai kemampuan sistem untuk mendeteksi kegagalan sebelum terjadi dampak[9]. (Lihat **Gambar 1**, tahap ketiga).

4. RPN (S x O x D)

Risk Priority Number (RPN) adalah angka yang dihasilkan dari mengalikan nilai Severity, Occurrence, dan Detection (S x O x D), yang memberikan indikasi prioritas risiko yang harus ditangani. RPN digunakan untuk mengidentifikasi risiko paling signifikan dalam sistem sehingga langkah-langkah mitigasi dapat diterapkan secara efisien[9]. (Lihat **Gambar 1**, tahap keempat).

5. Prioritas Risiko

Risiko dalam konteks sistem informasi mengacu pada kemungkinan terjadinya peristiwa yang dapat mempengaruhi keberhasilan proyek atau operasi sistem. Risiko dapat berupa kegagalan teknis, kesalahan manusia, atau perubahan dalam kebutuhan pengguna, dan harus dikelola dengan strategi yang tepat untuk meminimalkan dampak negatif. Prioritas risiko merupakan proses yang berguna untuk menentukan mana risiko yang harus ditangani terlebih dahulu berdasarkan tingkat keparahan dan kemungkinan terjadinya. Dalam konteks sistem informasi, penentuan prioritas risiko membantu tim untuk fokus pada masalah yang paling kritis yang dapat mempengaruhi keberhasilan proyek atau operasi sistem[10]. (Lihat Gambar 1, tahap kelima).

6. Rekomendasi

Rekomendasi merupakan langkah-langkah yang diusulkan untuk mengurangi risiko yang telah diidentifikasi dalam analisa. Rekomendasi ini biasanya mencakup perubahan dalam desain sistem, peningkatan pelatihan pengguna, atau penambahan fitur pemantauan untuk mendeteksi masalah secara lebih awal.[10]. (Lihat **Gambar 1**, tahap keenam).

HASIL DAN PEMBAHASAN

1. Analisa Sistem

a. Menentukan Objek dan Subjek Penelitian

1) Objek Penelitian

Objek penelitian adalah fokus utama yang diteliti dan dianalisis, dimana data akan dikumpulkan. Dalam penelitian ini, objek penelitian adalah:

a) Website Sistem Informasi Pelayanan Administrasi Surat Menyurat (SIASY):
Website ini berfungsi sebagai platform untuk mengelola dan memproses administrasi surat menyurat. Penelitian akan menganalisis berbagai aspek dari website ini, termasuk arsitektur sistem, fungsi yang ada, dan interaksi pengguna.

b) Analisis Risiko IT:
Proses dan praktik yang diterapkan untuk mengidentifikasi, menganalisis, dan mengelola risiko yang terkait dengan teknologi informasi pada website SIASY. Penelitian akan mengkaji bagaimana risiko diidentifikasi dan dikelola, serta efektivitas pendekatan yang digunakan.

c) Metode FMEA (Failure Mode and Effects Analysis):
Metode yang diterapkan untuk menganalisis hal yang kurang beserta potensi kegagalan dalam sistem dan dampaknya. Penelitian ini akan mengaplikasikan FMEA untuk mengidentifikasi mode kegagalan yang bisa saja terjadi pada website SIASY dan menghasilkan rekomendasi untuk mitigasi.

2) Subjek Penelitian

Subjek dalam penelitian ini yaitu Admin SIASY, Kepala sub bagian koordinator, Dosen, dan Mahasiswa.

Berikut adalah tabel RACI yang menunjukkan peran dan tanggung jawab dalam konteks analisis dampak risiko IT pada website Sistem Informasi Pelayanan Administrasi Surat Menyurat (SIASY):

Tabel 1. RACI

Tugas/Proses	Admin	Kepala Sub Koordinator	Dosen	Mahasiswa
Identifikasi masalah sistem	R	A	C	I
Pengumpulan data dan analisis risiko	R	A	C	I
Penerapan metode FMEA	R	A	C	I
Pengembangan dan implementasi solusi	R	A	C	I
Pemantauan dan evaluasi sistem	R	A	C	I
Komunikasi hasil analisis risiko	R	A	C	I
Penyusunan laporan manajemen risiko	R	A	C	I
Pelatihan pengguna mengenai sistem	R	A	C	I
Tindak lanjut terhadap umpan balik	R	A	C	I

Keterangan:

a. R (Responsible): Pihak yang bertanggung jawab langsung untuk menyelesaikan tugas. Dalam hal ini, Admin SIASY bertanggung jawab untuk semua tugas yang terkait dengan pengelolaan risiko IT[11].
b. A (Accountable): Pihak yang memiliki tanggung jawab akhir dan otoritas untuk keputusan. Kepala Bagian bertanggung jawab untuk memastikan bahwa semua tugas dilakukan dengan baik[11].
c. C (Consulted): Pihak yang dikonsultasikan, memberikan masukan atau saran. Dosen terlibat dalam memberikan umpan balik yang relevan[11].
d. I (Informed): Pihak yang harus diinformasikan tentang kemajuan dan hasil. Mahasiswa diinformasikan mengenai perubahan atau kebijakan terkait sistem[11].

b. Pengumpulan data

Data yang digunakan dalam penelitian ini merupakan data primer yang diperoleh secara langsung melalui pengamatan terhadap objek yang diteliti. Selanjutnya, dilakukan wawancara dan distribusi kuesioner.

Wawancara: Mengadakan sesi tanya jawab dengan admin SIASY untuk mendapatkan informasi mendalam mengenai topik penelitian.

Berikut adalah daftar wawancara yang kami lakukan:

1. Tahun berapa website di bangun?
2. Apa tujuan utama website?

3. Apakah pernah ada masalah terkait IT pada website?
4. Berapa jumlah populasi pengguna?
5. Siapa saja yang menggunakan website?
6. Siapa yg paling sering menggunakan website?
7. Bagaimana prosedur fakultas dalam mengelola risiko IT pada website?
8. Apakah fakultas memiliki tim khusus dalam mengelola risiko IT
9. Apa saja risiko utama yang pernah teridentifikasi dalam penggunaan website?
10. Apakah fakultas pernah menggunakan FMEA atau metode lain dalam manajemen resiko IT?
11. Apakah ada tantangan terbesar yg dihadapi dalam mengelola risiko IT?
12. Apakah fakultas pernah mengalami insiden keamanan yg signifikan pada website?
13. Bagaimana proses evaluasi dan pemantauan keamanan IT dilakukan pada website?
14. Apakah ada standar/kebijakan khusus dari fakultas terkait manajemen risiko IT?

Kuesioner: Menyebarkan kuesioner kepada RACI yang berisi pertanyaan terstruktur kepada responden untuk mendapatkan data kuantitatif.

c. Pengolahan data

Langkah selanjutnya dalam analisis data adalah menentukan satuan untuk variabel occurrence, severity, dan detection. Umumnya, karena metode FMEA lebih sering diterapkan dalam bidang teknik industri, semua variabel tersebut diukur berdasarkan satuan produksi. Namun, dalam penelitian ini, yang berfokus pada sistem informasi, satuan yang digunakan akan disesuaikan. Nilai untuk variabel occurrence, severity, dan detection adalah skala ordinal dari 1 hingga 10, menurut Hariyanti, F., & Cholifah, C. (2024).

Teknik untuk menghitung skala penilaian Severity, Occurrence, dan Detection (SOD) dalam analisis Failure Mode and Effects Analysis (FMEA) melibatkan beberapa langkah kunci. Pertama, tentukan kriteria penilaian untuk masing-masing kategori, dengan Severity yang mencerminkan dampak kegagalan, Occurrence yang menunjukkan frekuensi terjadinya, dan Detection yang menilai kemampuan mendeteksi kegagalan. Selanjutnya, kumpulkan data dari tim multidisiplin dan lakukan penilaian untuk setiap mode kegagalan, kemudian hitung Risk Priority Number (RPN) dengan mengalikan nilai S, O, dan D. Mode kegagalan diurutkan berdasarkan nilai RPN untuk mengidentifikasi prioritas risiko, diikuti dengan diskusi tentang langkah-langkah mitigasi yang diperlukan. Dokumentasikan hasil dan lakukan pemantauan berkala untuk menilai efektivitas tindakan yang diambil[17].

Berikut adalah tabel yang menunjukkan satuan masing-masing ukuran skala tersebut:

Tabel 2. Skala Penilaian Severity

Skala	Keterangan
1	**Negligible severity** (Dampak yang dapat diabaikan). Kita tidak perlu khawatir bahwa dampak ini akan mempengaruhi kualitas produk, dan pengguna mungkin tidak akan menyadari cacat ini.
2,3	**Mild severity** (Dampak yang ringan). Dampak yang ditimbulkan bersifat ringan, sehingga pengguna tidak akan merasakan penurunan kualitas..
4,5,6	**Moderate severity** (Dampak yang sedang). Pengguna akan merasakan penurunan kualitas, tetapi masih dalam batas toleransi.
7,8	**High severity** (Dampak yang tinggi). Pengguna akan merasakan penurunan kualitas yang melebihi batas toleransi.

Skala	Keterangan
9,10	**Potential severity** (Dampak yang sangat tinggi). Dampak yang ditimbulkan sangat signifikan terhadap kualitas lainnya, dan pengguna tidak akan menerima hal tersebut.

Tabel 3. Skala Penilaian Occurence

Skala	Degree
1	Remote
2,3	Low
4,5,6	Moderate
7,8	High
9,10	Very High

Tabel 4. Skala Penilaian Detection

Skala	Keterangan
1	Metode deteksi dan pencegahan sangat efektif, sehingga hampir tidak ada peluang bagi penyebab kegagalan untuk muncul.
2,3	Peluang terjadinya penyebab sangat rendah.
4,5,6	Peluang terjadinya penyebab bersifat moderat. Metode pencegahan terkadang memungkinkan terjadinya penyebab tersebut.
7,8	Peluang terjadinya penyebab masih tinggi. Metode pencegahan kurang efektif, sehingga penyebab masih dapat terjadi kembali.
9,10	Peluang terjadinya penyebab sangat tinggi. Metode deteksi dan pencegahan sangat tidak efektif, dan penyebab terus berulang.

2. Hasil analisis potensi kegagalan

Hasil ini diperoleh dari hasil wawancara beserta kuesioner yang disebarkan kepada anggota RACI, yang memiliki untuk mengumpulkan informasi dan data tentang pandangan serta pengalaman mereka terkait topik yang diteliti. Kuesioner tersebut dirancang untuk menggali berbagai aspek dan mendapatkan perspektif yang komprehensif dari responden, sehingga hasilnya dapat memberikan wawasan yang lebih mendalam tentang isu yang dihadapi.

1. Identifikasi Mode Kegagalan

Berdasarkan hasil wawancara, ada beberapa mode kegagalan yang dapat diidentifikasi adalah:

a. Sistem Tidak Sinkron: Pengguna melaporkan bahwa sistem tidak sinkron dengan sistem keuangan, yang dapat menyebabkan masalah dalam pemrosesan pembayaran UKT. Hal ini menunjukkan adanya risiko terkait integrasi sistem
b. Akses Tidak Terkontrol: Mahasiswa yang alpa studi masih bisa mengakses sistem, yang seharusnya dibatasi. Ini menciptakan risiko penyalahgunaan akses dan informasi.
c. Kurangnya Tim Khusus untuk Manajemen Risiko IT: Pengalaman sebelumnya dengan server yang down menunjukkan potensi risiko gangguan operasional yang dapat mengakibatkan downtime dan ketidakpuasan pengguna
d. Ketidakjelasan dalam Prosedur Pengelolaan Risiko: Ketidakjelasan dalam prosedur pengelolaan risiko dapat mengakibatkan konsekuensi serius bagi organisasi, termasuk kesulitan dalam pengambilan keputusan dan peningkatan potensi kerugian. Salah satu penyebab utama ketidakjelasan ini adalah kurangnya standarisasi dalam prosedur yang diterapkan, yang dapat menyebabkan kebingungan di antara karyawan mengenai langkah-langkah yang harus diambil dalam situasi tertentu

3. Menentukan Severity, Occurrence, Detection, dan Hasil Perhitungan RPN

Untuk menentukan Risk Priority Number (RPN) berdasarkan hasil wawancara dan kuesioner analisis risiko yang telah dilakukan, kita perlu menilai setiap mode kegagalan dengan tiga komponen: Severity (S), Occurrence (O), dan Detection (D). Setiap komponen dinilai pada skala 1 hingga 10, di mana:

1. **Severity (S)**: Mengukur dampak dari kegagalan jika terjadi **(**1 = tidak berdampak; 10 = dampa**k** sangat serius).
2. **Occurrence (O)**: Mengukur frekuensi terjadinya kegagalan (1 = sangat jarang; 10 = sangat sering).
3. **Detection (D)**: Mengukur kemampuan untuk mendeteksi kegagalan sebelum dampak terjadi (1 = sangat baik; 10 = sangat buruk).

Rumus menghitung RPN:

$$RPN = S \times O \times D \quad (1)$$

Tabel 5. Perhitungan RPN

Mode Kegagalan	S	O	D	RPN
Sistem Tidak Sinkron	8	7	6	336
Akses Tidak Terkontrol	9	6	5	270
Kurangnya Tim Khusus untuk Manajemen Risiko IT	7	5	4	140
Ketidakjelasan dalam Prosedur Pengelolaan Risiko	5	5	7	175

Tabel 6. Prioritas Risiko

Mode Kegagalan	S	O	D	RPN
Sistem Tidak Sinkron	8	7	6	336
Akses Tidak Terkontrol	9	6	5	270
Ketidakjelasan dalam Prosedur Pengelolaan Risiko	5	5	7	175
Kurangnya Tim Khusus untuk Manajemen Risiko IT	7	5	4	140

Dari analisis diatas, mode kegagalan yang paling kritis adalah **Sistem Tidak Sinkron** dengan RPN tertinggi 336, diikuti oleh **Akses Tidak Terkontrol** dengan RPN 270. Ini menunjukkan bahwa kedua masalah ini harus menjadi prioritas utama dalam manajemen risiko IT di website SIASY. Tindakan mitigasi yang tepat harus segera diterapkan untuk mengurangi risiko yang terkait dengan mode kegagalan tersebut.

4. Hasil Rekomendasi

Dari perhitungan RPN dan prioritas risiko yang sudah didapat selanjutnya memberikan rekomendasi agar penggunaan sistem dan proses yang ada pada website Sistem Informasi Pelayanan Administrasi Surat Menyurat (SIASY) dapat berjalan dengan lancar. Berikut tabel Rekomendasi:

Tabel 7. Rekomendasi

Risiko	Rekomendasi
Sistem Tidak Sinkron	Melakukan audit sistem untuk mengidentifikasi dan memperbaiki masalah integrasi antara sistem, dan Mengembangkan protokol komunikasi yang lebih baik antara sistem keuangan dan sistem akademik[13].
Akses Tidak Terkontrol	Mengimplementasikan kontrol akses berbasis peran untuk membatasi akses mahasiswa yang tidak aktif, dan Melakukan audit rutin terhadap hak akses pengguna untuk memastikan kepatuhan terhadap kebijakan[14].
Kurangnya Tim Khusus untuk Manajemen Risiko IT	Membentuk tim manajemen risiko IT yang terdiri dari anggota yang memiliki keahlian teknis dan manajerial, serta menyediakan pelatihan dan sumber daya yang diperlukan agar tim dapat mengelola risiko secara efektif[15].
Ketidakjelasan dalam Prosedur Pengelolaan Risiko	Mengembangkan dan mendokumentasikan prosedur pengelolaan risiko yang jelas dan terstandarisasi[16].

KESIMPULAN

Penelitian situs web Sistem Informasi Layanan Administrasi Surat (SIASY) tentang manajemen risiko TI yang menggunakan metode FMEA telah menghasilkan wawasan yang komprehensif tentang tantangan dan potensi risiko yang dihadapi. Kesimpulan utama, yang diperoleh dari wawancara dan hasil analisis risiko adalah sebagai berikut:

1. **IdentifikasiModeKegagalan**:
   Empat mode kegagalan utama telah diidentifikasi: kurangnya sinkronisasi dalam sistem, akses tidak terkendali, tidak adanya tim khusus untuk manajemen risiko TI, dan prosedur manajemen risiko yang tidak jelas. Masing-masing mode kegagalan yang diidentifikasi ini secara substansial mempengaruhi keandalan dan efektivitas sistem.
2. **AnalisisRisiko**:
   RPN yang dihitung menunjukkan bahwa mode kegagalan "sistem tidak sinkron" memegang prioritas tertinggi dengan RPN 336, sementara "akses tidak terkontrol" dengan RPN 270. Ini menandakan bahwa kedua masalah ini harus menjadi penekanan utama dalam manajemen risiko.
3. **PenyebabKegagalan**:
   Integrasi sistem yang lemah, pengaturan akses yang tidak jelas, infrastruktur TI yang tidak memadai, dan tidak adanya tim khusus untuk mengelola risiko TI merupakan faktor-faktor yang menyebabkan kegagalan. Selain itu, prosedur manajemen risiko yang tidak jelas juga berperan dalam masalah ini.
4. **RekomendasiMitigasi**:
   Sangat penting untuk menerapkan strategi mitigasi yang jelas, yang harus melibatkan pembentukan tim khusus yang berfokus pada manajemen risiko, menciptakan kebijakan kontrol akses yang lebih ketat, dan meningkatkan infrastruktur TI. Selain itu, memastikan sinkronisasi data melalui integrasi sistem keuangan dengan SIASY juga sangat penting.
5. **PentingnyaManajemenRisiko**:
   Penelitian ini menekankan bahwa manajemen risiko yang efektif merupakan faktor krusial dalam meningkatkan keandalan sistem informasi dan memperkuat kepercayaan pengguna. Dengan mengidentifikasi dan mengurangi risiko secara aktif, fakultas dapat menjamin bahwa sistem SIASY beroperasi dengan sebaik-baiknya dan memberikan layanan berkualitas kepada pengguna.

Penelitian ini memberikan dasar yang kuat untuk kemajuan manajemen risiko TI dalam fakultas, yang berfungsi sebagai referensi berharga untuk keputusan strategis terkait peningkatan sistem. Dengan mengadopsi rekomendasi yang sesuai, diharapkan risiko saat ini dapat dikurangi, sehingga meningkatkan kualitas layanan administrasi surat menyurat di fakultas.

DAFTAR PUSTAKA

[1] Baskoro, D. A., Maipita, I., Fitrawaty, F., & Dongoran, F. R. (2023). Digitalisasi Sistem Informasi dan Administrasi Desa Sebagai Upaya Menuju Desa Cerdas di Desa Kolam, Percut Sei Tuan, Deli Serdang, Sumatera Utara. *Dinamisia: Jurnal Pengabdian Kepada Masyarakat*, *7*(3), 624-635.)

[2] Rahmawita, M. T., Riswandi, R., Maita, I., & Zarnelly, Z. (2022). Analisis kepuasan mahasiswa dengan metode eucs dalam penggunaan SIASY fakultas tarbiyah dan keguruan. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, *8*(2), 201-209.

[3] Megawati, M., & Hamzah, M. L.(2022) Analisis Manajemen Risiko Keamanan Sistem BMKGSoft Menggunakan Metode OCTAVE-S. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, *8*(1), 62-67.

[4] Munaroh, L., Amrozi, Y., & Nurdian, R. A. (2021). Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001: 2013. *Technomedia Journal*, *5*(2 Februari), 167-181.

[5] Gagas, R. J., Syah, I., & Febryanto, F. (2021). Analisis, Evaluasi, Dan Mitigasi Risiko Aset Teknologi Informasi Menggunakan Framework Octave Dan Fmea (Studi Kasus: Unit Pengelola Teknis Teknologi Informasi Dan Komunikasi Universitas Xyz). *Jurnal Khatulistiwa Informatika*, *9*(2).

[6] Purwati, N., & Wibowo, H. (2021). Transformasi Layanan Administrasi Akademik di Perguruan Tinggi . *TEKNIKA*, *15*(1), 23-31.

[7] Yamalia, I., & Siagian, S. (2019). Analisa Sistem Informasi Pengolahan Data Nilai Siswa Berbasis Web. *Journal V-Tech*, *2*(1), 286633.

[8] Arifianto, E. Y., & Briliana, R. N. (2021, December). Identifikasi Penyebab dan Analisis Risiko Kegagalan Proses Produksi Geomembrane Pabrik Plastik Menggunakan Pendekatan FMEA. In *Seminar Nasional Teknik dan Manajemen Industri* (Vol. 1, No. 1, pp. 66-72).

[9] Nelfiyanti, N., Setiawan, B., & Setiawan, A. (2024). Analisis Faktor Keterlambatan Pengiriman Produk Ke Konsumen Dengan Menggunakan Metode Fmea Pt. Mrp. *Prosiding Semnastek*.

[10] Kurniawan, G. I., Disman, D., Hurriyati, R., & Dagustani, D. (2021). Penentuan Prioritas Risiko Melalui Analytical Hierarchy Process (Ahp) Sebagai Upaya Pengembangan Potensi Kawasan Wisata Pantai Jawa Barat Selatan. *Jurnal Inovasi Penelitian*, *1*(10), 2057-2068.

[11] Yogantara, S. E., Puspita, I. A., & Widyasthana, S. (2022). Perancangan Sistem Task Management menggunakan Raci Matriks dalam Tampilan Dashboard pada Proyek Pembuatan Feasibility Study dan Master Plan Rumah Sakit. *Jurnal Pendidikan dan Konseling (JPDK)*, *4*(5), 2132-2143.

[12] Hariyanti, F., & Cholifah, C. (2024). Reducing Pending BPJS Claims Through Risk Management. *Academia Open*, *9*(1), 10-21070.

[13] Rahayu, T., Matondang, N., & Hananto, B. (2020). Audit Sistem Informasi Akademik Menggunakan Metode Cobit 5. Jurnal Teknologi Informasi dan Pendidikan, 13(1), 117-123.

[14] Yushita Marini, S. E., Rihfenti Ernayani, S. E., Ak, M., Taufik Rachman, S. E., Bakri, A. A., SE, M., ... & SE, M. A. (2024). *SISTEM INFORMASI AKUNTANSI*. Cendikia Mulia Mandiri.

[15] Rajjani, J. S. A., Hanggara, B. T., & Musityo, Y. T. (2021). Evaluasi Manajemen Risiko Teknologi Informasi pada Department of ICT PT Semen Indonesia (Perseo) Tbk menggunakan Framework COBIT 2019 dengan Domain EDM03 dan APO12. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *5*(5), 1734-1744.

[16] Nur, F. R., & Wulandari, T. S. (2022). Analisis manajemen risiko pembiayaan murabahah dalam meningkatkan profitabilitas perspektif manajemen syariah (Studi kasus BPR Syariah Artha Mas Abadi). *AT-TAWASSUTH: Jurnal Ekonomi Islam*, *7*(2), 235-253.

[17] Gambino, A. A. M. (2018). Penerapan Failure Mode and Effect Analysis (FMEA) Dan Diagram Fishbone Pada Percetakan PT. Pandji Media Gemilang. *Ungraduate Program Management*.