Jurnal Sistem Informasi, Manajemen, dan Akuntansi (SIMAK)
Volume 22 Issue 01, May 2024
P-ISSN: 1693-5047, E-ISSN: 2621-0320

Risk Mitigation of Academic Information System in XYZ University

Muhammad Haris Fadhillah[1]
Faculty of Science and Technology, Indonesian Cooperative University

Abstract: *Academic information system (AIS) is an asset that universities must have to facilitate the work of operators and services to students. Nowadays, there are several threats faced by AIS managers related to data and information storaged security, thus requiring good risk management to mitigate risks that arise in the future. This research uses the fault tree analysis (FTA) and failure mode effect analysis (FMEA) methods to mitigate risks that may occur in AIS. The results show that there are 9 potential risks with 18 risk impacts, of which 1 risk impact is categorized as high, 4 risks are categorized as medium, and 13 risks are categorized as low. Five risk impacts that are categorized as high and medium need to be further evaluated, there are computer failure (R1), computer viruses (R2), external parties breaking into AIS (R7), capacity being full (R9), and server failure (R11).*
Keywords: Risk Mitigation, Fault Tree Analysis (FTA), Failure Mode Effect Analysis (FMEA), Information System

Article Info:
Received: January 23th, 2024 | Revised: April 17th, 2024 | Accepted: May 27th, 2024
DOI: 10.35129/simak.v22i01.480

[1] *E-mail: haris.irhamna@gmail.com (Correspondence Author)*

Mitigasi Risiko Sistem Informasi Akademik pada Universitas XYZ

Muhammad Haris Fadhillah
Fakultas Sains dan Teknologi, Universitas Koperasi Indonesia

Abstrak: Sistem informasi akademik (SIA) merupakan aset yang wajib dimiliki oleh perguruan tinggi untuk memudahkan pekerjaan operator dan pelayanan kepada mahasiswa. Saat ini, terdapat beberapa ancaman yang dihadapi pengelola SIA yang berkaitan dengan keamanan data dan informasi yang disimpan, sehingga membutuhkan manajemen risiko yang baik untuk memitigasi risiko-risiko yang timbul di masa yang akan datang. Pada penelitian ini menggunakan metode *fault tree analysis* (FTA) dan *failure mode effect analysis* (FMEA) untuk memitigasi risiko-risiko yang mungkin terjadi pada SIA. Hasil penelitian menunjukkan terdapat 9 potensi risiko dengan 18 dampak risiko, yang aman 1 dampak risiko terkategori tinggi, 4 risiko terkategori sedang, dan 13 risiko terkategori rendah. Lima dampak risiko yang terkategori tinggi dan sedang perlu dievaluasi lebih lanjut yaitu komputer mati (R1), virus komputer (R2), pihak eksternal membobol SIA (R7), kapasitas yang ditampung sudah penuh (R9), dan server mati (R11).
Kata-kata Kunci: Mitigasi Risiko, *Fault Tree Analysis* (FTA), *Failure Mode Effect Analysis* (FMEA), Sistem Informasi

1. PENDAHULUAN

Sistem informasi akademik (SIA) memiliki peran yang sangat penting dalam mengumpulkan beberapa data terkait dengan proses pendidikan di perguruan tinggi meliputi data-data dosen dan mahasiswa seperti rekapitulasi kehadiran, nilai mata kuliah, transkrip, catatan keuangan dan catatan-catatan historis mahasiswa-mahasiswa yang telah lulus (Aswati *et al*., 2015; Purwanto, 2017). Saat ini, SIA merupakan suatu aset yang mutlak untuk dimiliki agar dapat mempermudah pekerjaan pihak administrasi serta memudahkan mahasiswa dalam mendapatkan pelayanan yang lebih efisien (Irawan, 2018). Salah satu perguruan tinggi yang menerapkan SIA yang dimaksud adalah Universitas XYZ dengan nama PUSLIAT yang merupakan singkatan dari Pusat Layanan Informasi Akademik Terpadu.

Kemudahan pelayanan melalui SIA diiringi dengan kemudahan pengaksesan data dan informasi yang telah disimpan, dengan arti lain data dan informasi yang dikelola dapat disalahgunakan oleh pihak-pihak yang tidak bertanggungjawab sehingga dapat mengganggu proses pekerjaan layanan akademik (Chrisanty dan Tambotoh, 2023). Sebagai aset penting bagi perguruan tinggi, keamanan informasi pada SIA sangat dibutuhkan untuk dilindungi dan diamankan untuk menjamin ketersediaan informasi yang berguna dan dapat dipercaya baik oleh lingkungan internal maupun eksternal (Nugraha dalam Kholifah *et al.*, 2021).

Dalam meminimalisir kejadian-kejadian tersebut, Universitas XYZ memerlukan pencegahan-pencegahannya (mitigasi) melalui pengelolaan manajemen risiko yang baik dimulai dari mengidentifikasi risiko, menganalisis risiko, dan mengevaluasi risiko yang mungkin akan terjadi pada SIA. Penelitian yang berkaitan dengan mitigasi risiko pada sistem informasi telah dilakukan oleh beberapa peneliti dengan metode-metode yang berbeda-beda, diantaranya menggunakan metode *OCTAVE Allegro* (Supradono, 2009; Jakaria dan Dirgahayu, 2013; Kuntari *et al.*, 2018; Matondang *et al.*, 2018; Deva dan Jayadi, 2022), *Failure Mode Effect Analysis* (FMEA)*, Framework NIST SP 800-30* (Nurochman, 2014; Nugraha, 2016; Hardani dan Ramli, 2022)*, Framework ISO27001,* dan *Framework ISO31000* (Ramdhany dan Krisdiawan, 2018; Wahyuari dan Sidik, 2023). Namun, ada juga yang mengkombinasikan beberapa metode yang telah disebutkan seperti *OCTAVE Allegro* dengan FMEA (Setyadi dan Kusumawati, 2016; Putri dan Kusumawati, 2017; Gagas *et al.,* 2021), dan *OCTAVE Allegro* dengan *Framework ISO27001* (Wijayanti 2018; Anshori *et al.*, 2019).

Sedangkan pada penelitian ini akan menggunakan kombinasi dua metode yaitu metode FMEA dan *fault tree analysis* (FTA) untuk mengidentifikasi, menganalisis, serta mengevaluasi risiko yang terdapat pada SIA Universitas XYZ. Hingga saat ini belum ada penelitian yang menggunakan FTA untuk memitigasi risiko sistem informasi, terlebih khusus pada sistem informasi akademik. FTA merupakan suatu teknik yang digunakan untuk mengidentifikasi risiko yang berperan untuk mengidentifikasi risiko yang berperan terhadap terjadinya kegagalan (Hanif *et al.*, 2015).

Berdasarkan hal tersebut, maka perlu dilakukan penelitian tentang mitigasi risiko sistem informasi akademik menggunakan metode *failure mode effect analysis* dan *fault tree analysis* di Universitas XYZ. Penelitian ini bertujuan untuk memberikan gambaran mengenai manajemen risiko sistem informasi akademik di Universitas XYZ dalam mengidentifikasi, menganalisis, dan mengevaluasi risiko dengan menggunakan metode FMEA dan FTA serta untuk mengetahui faktor-faktor apa yang mempengaruhi pelaksanaan manajemen risiko di sistem informasi akademik. Metode FTA digunakan untuk mengidentifikasi risiko-risiko yang akan ditemukan pada sistem informasi akademik, yang kemudian identifikasi risiko-risiko tersebut akan dianalisis serta dievaluasi menggunakan FMEA.

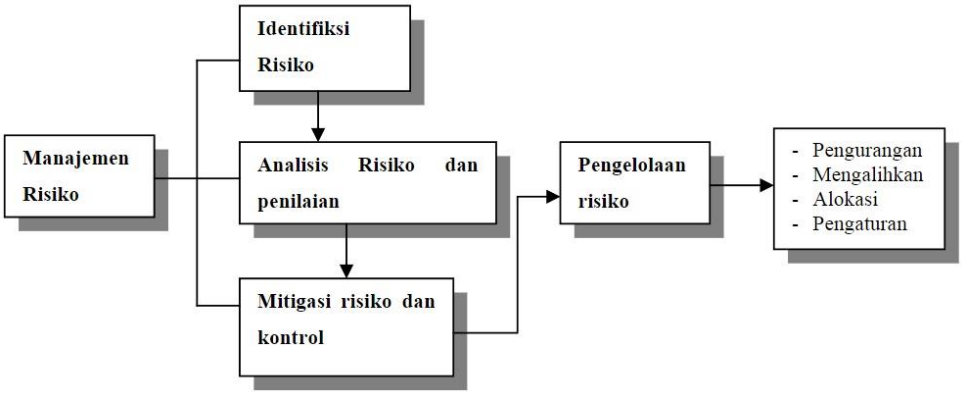
2. TINJAUAN LITERATUR

Manajemen Risiko

Risiko adalah akibat negatif dari sebuah kejadian atau suatu keputusan yang diambil dari kehidupan sehari-hari (Pinontoan dalam Nurochman, 2014). Pendapat lain mendefinisikan bahwa risiko sebagai kemungkinan akan terjadinya akibat buruk atau akibat yang merugikan, seperti kemungkinan kehilangan, cedera, kebakaran dan sebagainya (Darmawi, 2016). Sedangkan, menurut ISO 31000:2018 menyatakan bahwa risiko merupakan suatu ketidakpastian yang bisa berkonotasi negatif maupun positif yang berdampak pada tujuan yang ingin dicapai.

Sedangkan manajemen risiko merupakan suatu kegiatan yang dilaksanakan untuk mengidentifikasi, menganalisis, dan mengendalikan risiko yang mungkin terjadi dalam suatu aktivitas atau kegiatan sehingga akan diperoleh efektivitas dan efisiensi yang lebih tinggi (Darmawi, 2016). Penggunaan sistem informasi akademik tidak terlepas dari risiko, dikarenakan informasi merupakan suatu aset penting yang perlu dijaga kerahasiaannya untuk menghindari penyalahgunaan informasi yang diperoleh oleh pihak internal maupun eksternal yang tidak bertanggungjawab. Oleh sebab itu, maka pengelolaan risiko sistem informasi akademik diperlukan agar proses pelaksanaan layanan akademik berjalan dengan baik tanpa hambatan yang berarti.

Proses manajemen risiko menggarisbawahi sekurang-kurangnya 3 hal, yaitu identifikasi risiko, penilaian risiko, dan mengontrol serta meminimalisir risiko yang dapat dilihat pada gambar 1.



Gambar 1. Proses Manajemen Risiko
Sumber: Sandhyavitri dan Saputra (2019)

***Failure Mode Effect Analysis* (FMEA)**

FMEA adalah sebuah teknik rekayasa yang digunakan untuk menetapkan, mengidentifikasi, dan untuk menghilangkan kegagalan yang diketahui, permasalahan, error, dan sejenisnya dari sebuah sistem, desain, proses, dan atau jasa sebelum mencapai konsumen (Stamatis dalam Hanif *et al*., 2015). FMEA merupakan teknik evaluasi tingkat keandalan dari sebuah sistem untuk menentukan efek dari kegagalan dari sistem tersebut. Kegagalan digolongkan berdasarkan dampak yang diberikan terhadap kesuksesan suatu misi dari sebuah sistem. Secara umum, FMEA didefinisikan sebagai sebuah teknik yang mengidentifikasi tiga hal, diantaranya:

1) Penyebab kegagalan yang potensi dari sistem, desain produk, dan proses selama siklus hidupnya;
2) Efek dari kegagalan tersebut; dan
3) Tingkat kekritisan efek kegagalan terhadap fungsi sistem, desain produk, dan proses.

Adapun langkah-langkah dasar pengerjaan FMEA, yaitu (McDermott *et al.*, 2009):

1) Mengidentifikasi proses atau produk. Tim yang akan mengidentifikasi proses yang akan dianalisa, dapat mempertimbangkan *flowchart* untuk memudahkan identifikasi proses FMEA;
2) Menganalisis kemungkinan setiap potensi mode kegagalan yang berpotensi dapat terjadi;
3) Menganalisis efek yang ditimbulkan dari terjadinya setiap potensi kegagalan;
4) Menentukan peringkat dari *severity* (S), *occurrence* (O), dan *detection* (D) dengan skala penilaian dari 1 sampai 10;
5) Menghitung nilai *Risk Priority Number* (RPN) pada setiap potensi mode kegagalan dengan rumus:

   RPN = S x O x D .....(1)
6) Membuat daftar prioritas perbaikan untuk memperbaiki atau mencegah terjadinya potensi mode kegagalan; dan

7) Membuat analisis usulan perbaikan.

***Fault Tree Analysis* (FTA)**

FTA merupakan suatu teknik yang digunakan untuk mengidentifikasi risiko yang berperan terhadap terjadinya kegagalan (Hanif *et al*., 2015). Metode ini dilakukan dengan pendekatan *top-down*, yang diawali dengan asumsi kegagalan dari kejadian puncak (*top event*), kemudian merinci sebab-sebab suatu top event sampai pada suatu kegagalan dasar (*root cause*).

FTA merupakan metode yang efektif dalam menemukan inti permasalahan karena memastikan bahwa suatu kejadian yang tidak diinginkan atau kerugian yang ditimbulkan tidak berasal pada satu titik kegagalan. FTA mengidentifikasi hubungan antara faktor penyebab dan ditampilkan dalam bentuk pohon kesalahan yang melibatkan gerbang logika. Gerbang logika menggambarkan kondisi yang memicu terjadinya kegagalan, baik kondisi tunggal maupun kumpulan dari berbagai macam kondisi. Setiap kegagalan yang terjadi dapat digambarkan ke dalam suatu bentuk pohon analisa kegagalan dengan memindahkan komponen kegagalan ke dalam bentuk simbol (*logic transfer components*) dan FTA (Kuo, 2007).

Sebuah *fault tree* mengilustrasikan keadaan komponen-komponen sistem (*basic event*) dan hubungan antara *basic event* dengan *top event* menyatakan keterhubungan dalam gerbang logika. Adapun langkah-langkah FTA sebagai berikut:

1) Identifikasi *top level event*. Pada tahap ini diidentifikasi jenis kerusakan yang terjadi (*undesired event*) untuk mengidentifikasi kesalahan sistem. Pemahaman tentang sistem dilakukan dengan mempelajari semua informasi tentang sistem dan ruang lingkupnya;
2) Membuat diagram pohon kesalahan. Diagram pohon kesalahan menunjukkan bagaimana *top level events* bisa muncul pada jaringan;
3) Menganalisa pohon kesalahan. Analisa pohon kesalahan digunakan untuk memperoleh informasi yang jelas dari suatu sistem dan perbaikan yang diperlukan.

3. METODE PENELITIAN

Metode Penelitian yang Digunakan

Metode penelitian yang digunakan pada penelitian ini adalah metode studi kasus, dengan menggunakan pendekatan khusus dan mendalam melalui teknik wawancara kepada orang yang bersangkutan.

Data yang Diperlukan

Data yang diperlukan dalam penelitian ini yaitu data yang bisa menggambarkan masalah hingga mendapatkan gambaran objek penelitian. Adapun jenis data yang diperlukan dalam penelitian ini yaitu:

1) Data primer, yaitu data yang diperoleh secara langsung dengan cara berkomunikasi langsung dengan narasumber yang berhubungan dengan penelitian; dan

2) Data sekunder, yaitu data yang diperoleh secara tidak langsung seperti publikasi ilmiah, buku, dan laporan-laporan.

Sumber Data dan Teknik Pengumpulan Data

Sumber data yang diperlukan pada penelitian ini, diantaranya:

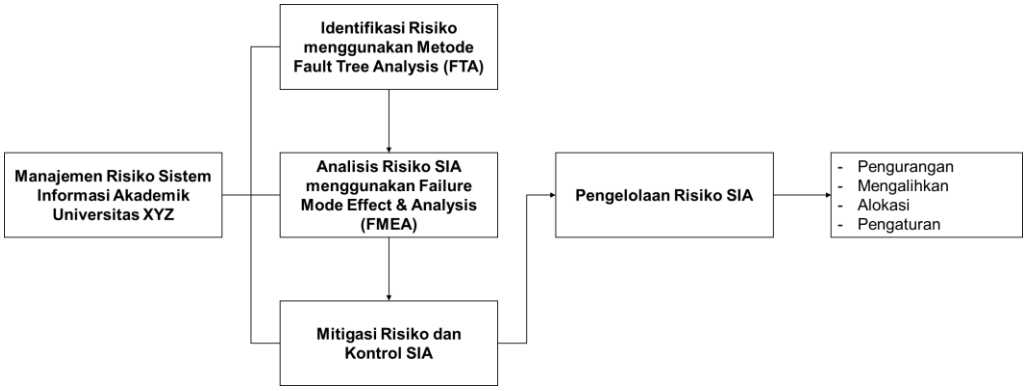
1) Informan, yaitu orang yang memberikan informasi terkait orang lain atau keadaan tertentu. Informan pada penelitian ini adalah pengelola SIA, operator SIA, dan mahasiswa selaku *user* SIA Universitas XYZ;
2) Lembaga, yaitu suatu organisasi yang mengumpulkan, menyimpan, dan menyediakan data, yaitu Universitas XYZ.

Sedangkan teknik pengumpulan data dilakukan dengan cara sebagai berikut:

1) Wawancara, yang dilakukan secara terstruktur maupun tidak terstruktur kepada informan melalui tatap muka maupun menggunakan jaringan komunikasi.
2) Studi pustaka, merupakan teknik pengumpulan data dengan cara mempelajari literatur-literatur yang berhubungan dengan masalah yang diteliti.

Analisis Data

Setelah mendapatkan data dan informasi, maka langkah selanjutnya yaitu mengolah data dan informasi agar menjadi data yang valid dan akurat. Secara ringkas, rancangan analisis data akan disajikan dalam Gambar 2.



Gambar 2. Rancangan Analisis Data Penelitian

Sumber: diolah Peneliti (2024)

Sedangkan ranalisis data secara sistematis akan dijabarkan sebagai berikut:

1) Mengidentifikasi Risiko yang mungkin akan Terjadi pada Sistem Informasi Akademik (SIA) di Universitas XYZ

Identifikasi risiko pada SIA akan dilakukan terlebih dahulu dengan metode *fault tree analysis* (FTA) agar dapat memperoleh gambaran yang jelas mengenai masalah-masalah yang mungkin akan terjadi berdasarkan hasil wawancara yang telah dilakukan kepada pengelola, operator, dan mahasiswa selaku pengguna SIA.

2) Menganalisis dan Menilai Risiko-risiko yang mungkin akan Terjadi pada SIA Berdasarkan Risiko yang telah Teridentifikasi

Setelah mengidentifikasi risiko dengan FTA, kemudian melakukan analisis dan penilaian risiko-risiko yang telah teridentifikasi menggunakan metode *failure mode effect analysis* (FMEA), dengan cara menentukan peringkat dari *severity* (S), *occurrence* (O), dan *detection* (D) dengan skala penilaian dari 1 sampai 10 guna menentukan nilai *risk priority number* (RPN) dengan rumus:

RPN = S x O x D .....(2)

Kriteria skala peringkat *severity*, *occurrence*, dan *detection* secara berurutan akan dirincikan pada tabel 1 sampai dengan tabel 3.

Tabel 1. Skala Peringkat *Severity* (S)

Dampak	Kriteria *Severity* (S)	Peringkat
Bahaya, Kegagalan terjadi tanpa ada peringatan	- Tidak sesuai dengan peraturan pemerintah - Menghentikan pengoperasian sistem produksi atau layanan jasa	10
Serius, Kegagalan terjadi dengan peringatan	- Tidak sesuai dengan peraturan pemerintah - Menghasilkan produk atau hasil jasa yang membahayakan konsumen	9
Ekstrem	- Mengganggu kelancaran sistem produksi atau layanan jasa - Produk tidak dapat dioperasikan (100% *scrap*) atau hasil jasa sangat tidak memuaskan (0% tingkat kepuasan)	8
Mayor	- Sedikit mengganggu kelancaran proses produksi atau layanan jasa - Kinerja produk tidak sempurna tetapi masih bisa difungsikan atau hasil jasa tidak cukup memuaskan tetapi masih bisa diterima konsumen	7
Signifikan	- Kinerja produk menurun karena beberapa fungsi tertentu mungkin tidak beroperasi atau kinerja hasil jasa menurun karena fungsi kenyamanan tidak terpenuhi	6
Sedang	- Kinerja produk atau hasil jasa menurun tetapi masih bisa diperbaiki	5
Rendah	- Kinerja produk atau hasil jasa menurun tetapi tidak memerlukan perbaikan	4
Kecil	- Dampak kecil terhadap sistem produksi atau layanan jasa atau kinerja produk atau hasil jasa – masih ada keluhan dari beberapa konsumen	3
Sangat Kecil	- Dampak sangat kecil terhadap sistem produksi atau layanan jasa atau kinerja produk atau hasil jasa – masih ada keluhan hanya dari konsumen tertentu	2
Tidak ada dampak	- Tidak ada dampak terhadap sistem produksi atau layanan jasa maupun produk atau hasil jasa	1

Sumber: dimodifikasi dari Alijoyo *et al.* (2021)

Tabel 2. Skala Peringkat *Occurrence* (O)

Peluang Terjadi Kegagalan	Tingkat Kemungkinan Kegagalan	Peringkat
Sangat tinggi dan ekstrem; kegagalan hampir tak terhindarkan	1 dari 2 Kemungkinan	10
Sangat tinggi; kegagalan berhubungan dengan proses yang gagal sebelumnya	1 dari 3 kemungkinan	9
Tinggi; kegagalan terus berulang	1 dari 8 kemungkinan	8
Relatif tinggi	1 dari 20 kemungkinan	7
Sedang cenderung tinggi	1 dari 80 kemungkinan	6
Sedang	1 dari 400 kemungkinan	5
Relatif rendah	1 dari 2.000 kemungkinan	4
Rendah	1 dari 15.000 kemungkinan	3
Sangat rendah	1 dari 150.000 kemungkinan	2
Hampir tidak mungkin terjadi kegagalan	1 dari 1.500.000 kemungkinan	1

Sumber: dimodifikasi dari Alijoyo *et al.* (2021)

Tabel 3. Skala Peringkat *Detect* (D)

Kemungkinan Kegagalan Terdeteksi	Kriteria *Detect* (D)	Peringkat
Hampir mustahil	Tidak ada kendali untuk mendeteksi potensi kegagalan	10
Sangat kecil	Terdapat sangat sedikit kendali untuk mendeteksi potensi kegagalan	9
Kecil	Terdapat sedikit terdapat kendali untuk mendeteksi potensi kegagalan	8
Sangat rendah	Terdapat kendali tetapi sangat rendah kemampuannya untuk mendeteksi potensi kegagalan	7
Rendah	Terdapat kendali tetapi rendah kemampuannya untuk mendeteksi potensi kegagalan	6
Sedang	Terdapat kendali yang memiliki kemampuan sedang/cukup untuk mendeteksi potensi kegagalan	5
Agak tinggi	Terdapat kendali yang memiliki kemampuan sedang cenderung tinggi untuk mendeteksi potensi kegagalan	4
Tinggi	Terdapat kendali yang memiliki kemampuan tinggi untuk mendeteksi potensi kegagalan	3
Sangat tinggi	Terdapat kendali yang memiliki kemampuan sangat tinggi untuk mendeteksi potensi kegagalan	2
Hampir pasti	Kendali hampir pasti dapat mendeteksi potensi kegagalan	1

Sumber: dimodifikasi dari Alijoyo *et al.,* (2021)

Setelah menentukan peringkat dari *severity, occurrence,* dan *detect,* maka akan dilakukan perhitungan RPN seperti yang telah dijabarkan. Hasil perhitungan RPN akan disesuaikan dengan kriteria yang tersaji pada tabel 4.

Tabel 4. Kriteria RPN

RPN	Kategori Kekritisan
501 – 1.000	Tinggi
251 – 500	Sedang
1 – 250	Rendah

Sumber: Alijoyo *et al.* (2021)

3) **Mengevaluasi Risiko-risiko yang Mungkin akan Terjadi pada SIA**
   Evaluasi risiko dilakukan berdasarkan hasil RPN yang telah diperoleh. Risiko-risiko yang akan dievaluasi adalah risiko-risiko yang termasuk dalam kategori tinggi dan sedang, sehingga risiko yang dikategorikan rendah akan dieliminasi untuk mempermudah menentukan prioritas penanganan dan kendali untuk setiap potensi kegagalan.
4) **Mitigasi Risiko-risiko yang Mungkin akan Terjadi pada SIA.**
   Mitigasi risiko berisikan strategi penanganan dan rekomendasi tindakan risiko untuk mengelola risiko yang akan terjadi berdasarkan hasil dari identifikasi, analisis, dan evaluasi risiko yang telah ditentukan sebelumnya.

4. HASIL DAN PEMBAHASAN

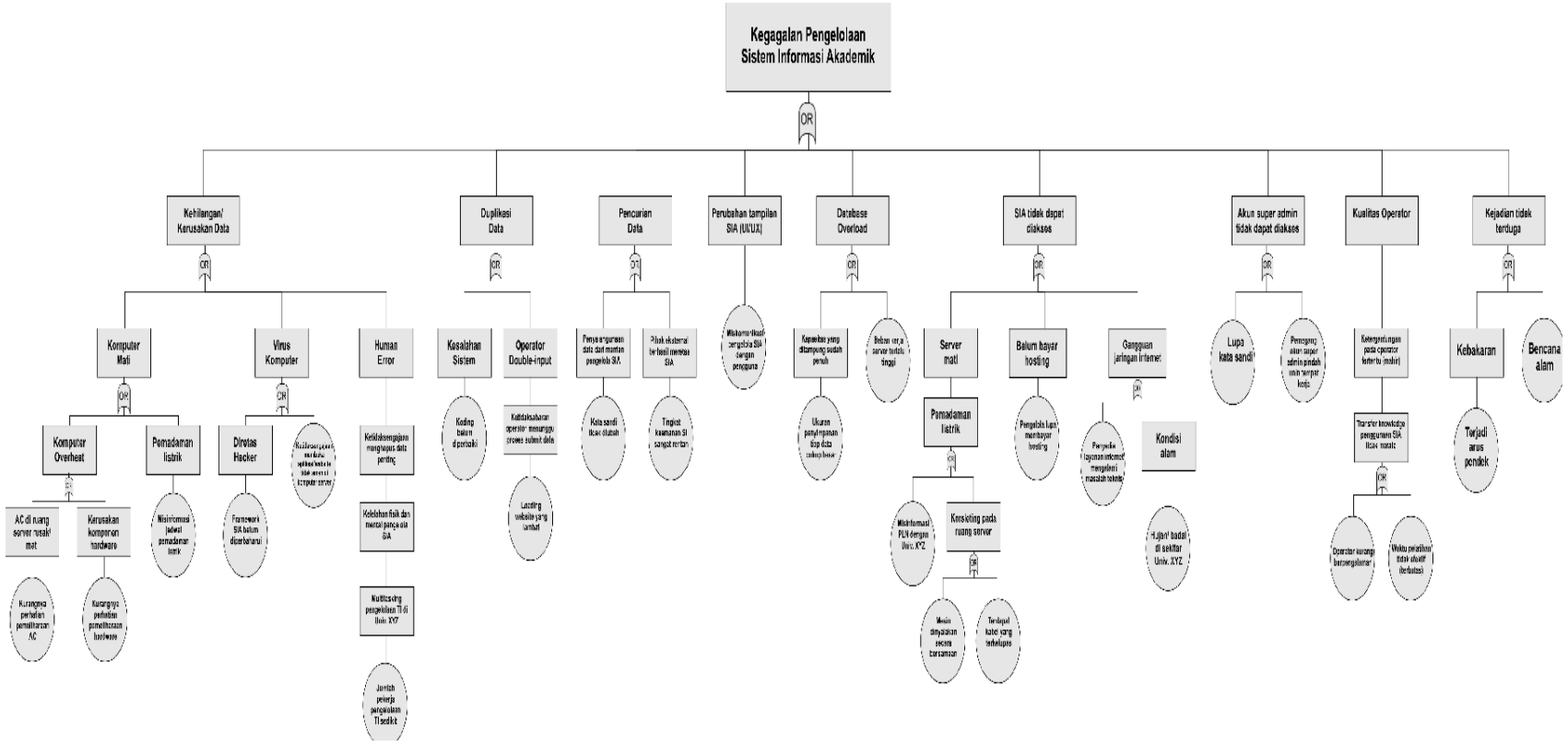
Identifikasi Risiko Sistem Informasi Akademik di Universitas XYZ

Identifikasi risiko bertujuan untuk menemukan, mengenali, dan mendeskripsikan kemungkinan risiko yang dapat mengakibatkan hambatan pada pengoperasian SIA. Identifikasi risiko diperoleh dengan cara melakukan wawancara terhadap pengelola, operator, dan mahasiswa sebagai pengguna SIA mengenai risiko yang berdampak negatif terhadap penggunaan SIA.

Setelah mengidentifikasi identifikasi risiko yang berpotensi pada kegagalan pengelolaan sistem informasi akademik, ditemukan beberapa potensi kegagalan sebagai berikut:

1) Kehilangan/ kerusakan data;
2) Duplikasi data;
3) Pencurian data;
4) Perubahan tampilan sistem informasi akademik (UI/UX);
5) Database overload;
6) SIA tidak dapat diakses;
7) Akun super admin tidak dapat diakses;
8) Kualitas operator; dan
9) Kejadian tidak terduga.

Berdasarkan beberapa potensi kegagalan diatas, maka ditelusuri lebih dalam beberapa faktor yang menyebabkan hal tersebut dengan menggunakan *fault tree analysis* (FTA) yang dapat dilihat pada gambar 3.



Gambar 3. ***Fault Tree Analysis***

Analisis dan Evaluasi Risiko Sistem Informasi Akademik di Universitas XYZ

Analisis risiko dilakukan dengan cara menghitung nilai *Risk Priority Number* (RPN). Sebelum menghitung RPN, ditentukan terlebih dahulu ranking untuk *severity* (S), *occurrence* (O), dan *detect* (D) berdasarkan wawancara yang telah dilakukan dengan informan. Tabel 5 berikut menyajikan hasil perhitungan RPN.

Tabel 5. Perhitungan RPN

Potensi Risiko	Dampak Risiko	Kode	S	O	D	RPN	Kategori
Kehilangan/kerusakan data	Komputer mati	R1	8	5	7	280	Sedang
	Virus komputer	R2	10	7	8	560	Tinggi
	Human error	R3	5	2	4	40	Rendah
Duplikasi data	Kesalahan sistem	R4	5	6	5	150	Rendah
	Operator *double-input*	R5	3	4	3	36	Rendah
Pencurian data	Penggunaan data dari mantan pengelola SIA	R6	6	5	6	180	Rendah
	Pihak eksternal membobol SIA	R7	10	6	8	480	Sedang
Perubahan tampilan SIA (UI/UX)	Misinformasi perubahan tampilan UI/UX SIA antara pengelola dengan pengguna SIA	R8	2	2	1	4	Rendah
Database overload	Kapasitas yang ditampung sudah penuh	R9	8	8	5	320	Sedang
	Beban kerja server terlalu tinggi	R10	7	4	5	140	Rendah
Sistem informasi akademik tidak dapat diakses	Server mati	R11	8	6	8	384	Sedang
	Belum bayar hosting	R12	8	3	2	48	Rendah
	Gangguan jaringan internet	R13	6	4	5	120	Rendah
Akun super admin tidak dapat diakses	Lupa kata sandi	R14	5	3	7	105	Rendah
	Pemegang akun super admin pindah unit atau tempat kerja	R15	8	1	9	72	Rendah
Kualitas operator	Ketergantungan pada operator yang mahir	R16	6	7	4	168	Rendah
Kejadian tidak terduga	Kebakaran	R17	10	2	8	160	Rendah
	Bencana alam	R18	10	2	10	200	Rendah

Sumber: Data diolah peneliti (2024)

Berdasarkan perhitungan pada tabel 5, diperoleh beberapa risiko SIA yang perlu dievaluasi lebih lanjut yaitu risiko yang terkategori sedang dan tinggi diantaranya komputer mati (R1), virus komputer (R2), pihak eksternal membobol SIA (R7), kapasitas yang ditampung sudah penuh (R9), dan server mati (R11).

Mitigasi Risiko Sistem Informasi Akademik di Universitas XYZ

Pada hasil analisis sebelumnya, terdapat empat risiko yang menjadi perhatian khusus diantaranya komputer mati (R1), virus komputer (R2), pihak eksternal membobol SIA (R7), kapasitas yang ditampung sudah penuh (R9), dan server mati (R11). Menurut informan, keempat risiko tersebut diyakini sangat mengganggu proses pengoperasian sistem informasi akademik di Universitas XYZ, sehingga diperlukan beberapa upaya-upaya mitigasi risiko dalam bentuk rekomendasi yang akan dijelaskan pada tabel 6.

Tabel 6. Mitigasi Risiko Sistem Informasi Akademik Universitas XYZ

Kode	Dampak Risiko	RPN	Kategori	Rekomendasi Penanganan
R1	Komputer mati	280	Sedang	1. Menginstall listrik cadangan khusus untuk ruang server; 2. Menjadwalkan pemeliharaan *(maintenance)* secara rutin untuk *hardware,* AC, dan perangkat lainnya pada ruang server, minimal 1 bulan sekali; 3. Melakukan manajemen kabel yang tertata rapi untuk menghindari korsleting dari kabel.
R2	Virus komputer	560	Tinggi	1. Meningkatkan keamanan komputer dan server melalui program anti-virus tertentu; 2. Membatasi url-url yang bisa diakses pada komputer server; 3. Memperbaharui tingkat keamanan sistem informasi akademik dengan bahasa-bahasa pemrograman terkini.
R7	Pihak eksternal membobol SIA	480	Sedang	1. Memperbaharui tingkat keamanan sistem informasi akademik dengan bahasa-bahasa pemrograman terkini; 2. Melakukan pergantian kata sandi secara rutin, minimal 1 bulan sekali.
R9	Kapasitas yang ditampung sudah penuh	320	Sedang	1. Menggunakan penyimpanan *cloud;* 2. Mengatur kapasitas file unggahan tertentu seminimal mungkin; 3. Membatasi format file unggahan dengan format tertentu seperti *pdf* dan *csv*.
R11	Server mati	384	Sedang	1. Menginstall listrik cadangan khusus untuk ruang server; 2. Menjadwalkan pemeliharaan *(maintenance)* secara rutin untuk *hardware,* AC, dan perangkat lainnya pada ruang server, minimal 1 bulan sekali; 3. Melakukan manajemen kabel yang tertata rapi untuk menghindari korsleting dari kabel.

Sumber: Data diolah peneliti (2024)

5. KESIMPULAN

Berdasarkan hasil dan pembahasan yang telah diuraikan, maka ditariklah beberapa kesimpulan, sebagai berikut:

1) Risiko-risiko yang teridentifikasi berdasarkan *fault tree analysis* yaitu 9 potensi risiko diantaranya yaitu kehilangan/kerusakan data, duplikasi data, pencurian data, perubahan tampilan sistem informasi akademik (UI/UX), database overload, SIA tidak dapat diakses, akun super admin tidak dapat diakses, kualitas operator, dan kejadian tidak terduga. Sedangkan 18 dampak risiko diantaranya yaitu komputer mati, virus komputer, *human error,* kesalahan sistem, operator *double-input,* penggunaan data dari mantan pengelola SIA, pihak eksternal membobol SIA, misinformasi perubahan tampilan UI/UX SIA antara pengelola dengan pengguna SIA, kapasitas yang ditampung sudah penuh, beban kerja server terlalu tinggi, server mati, belum bayar hosting, gangguan jaringan internet, lupa kata sandi, pemegang akun super admin pindah unit atau tempat kerja, ketergantungan pada operator yang mahir, kebakaran, dan bencana alam;
2) Analisis risiko berdasarkan hasil RPN menunjukkan terdapat 1 risiko yang terkategori tinggi, 4 risiko yang terkategori sedang, dan 13 risiko yang terkategori rendah;
3) Berdasarkan analisis risiko, terdapat 5 risiko yang harus dievaluasi lebih lanjut diantaranya R1, R2, R7, R9, dan R11;
4) Rekomendasi penanganan yang telah diberikan secara garis besar menunjukkan bahwa Universitas XYZ harus lebih memperhatikan kondisi ruang server untuk menjaga keberlangsungan sistem informasi akademik sebagai aset yang strategis.

Berdasarkan beberapa kesimpulan di atas, saran rekomendasi yang bermanfaat untuk digunakan dalam memitigasi risiko sistem informasi akademik di Universitas XYZ, sebagai berikut:

1) Perlunya pembuatan dokumentasi penilaian, evaluasi, dan mitigasi risiko untuk mengantisipasi berbagai ancaman risiko yang memberikan dampak negatif bagi pengelola SIA Universitas XYZ;
2) Pemahaman pengelola dan operator akan risiko yang mengancam sistem informasi akademik yang tidak terbatas dengan infrastruktur SI, tetapi memerlukan pemahaman teknis yang lain dalam bidang IT;
3) Diperlukan penelitian lebih lanjut mengenai manajemen risiko, seperti perilaku pengguna SIA dalam mengantisipasi ancaman risiko.

DAFTAR PUSTAKA

Jurnal/Buku:

Alijoyo, A., Wijaya, B., dan Jacob, I. (2021). Failure Mode Effect Analysis. *31 Teknik Penilaian Risiko Berbasis ISO 31010*. Bandung: Center for Risk Management & Sustainability (CRMS).

Anshori, F. A., Suprapto, dan Perdanakusuma, A, R. (2019). Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* 3(2), 1701–1707.

Aswati, S., Mulyani, N., Siagian, Y., dan Syah, A. Z. (2015). Peranan Sistem Informasi dalam Perguruan Tinggi. *Jurnal Teknologi dan Sistem Informasi,* 1(2), 79–86.

Chrisanty, T. W., dan Tambotoh, J. (2023). Analisis Manajemen Risiko Sistem Informasi Menggunakan ISO 31000:2018 di PT. XYZ. *ZONAsi: Jurnal Sistem Informasi,* 5(2), 371–380. https://doi.org/10.31849/zn.v5i2.13198

Darmawi, H. (2016). *Manajemen Risiko*. Jakarta: Bumi Aksara.

Deva, B. S., dan Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. *Jurnal Teknologi dan Informasi,* 12(2), 106–17. https://doi.org/10.34010/jati.v12i2.6829

Gagas, R. J., Syah, I. dan 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). https://doi.org/10.31294/jki.v9i2.11368

Hanif, R. Y., Rukmi, H. S., dan Susanty, S. (2015). Perbaikan Kualitas Produk Keraton Luxury di PT. X dengan Menggunakan Metode Failure Mode and Effect Analysis (FMEA) dan Fault Tree Analysis (FTA). *Reka Integra, Jurnal Online Teknik Industri,* 3(3), 137–147.

Hardani, M. S., dan Ramli, K. (2022). Perancangan Manajemen Risiko Keamanan Sistem Informasi Manajemen Sumber Daya dan Perangkat Pos dan Informatika (SIMS) Menggunakan Metode NIST 800-30. *JURIKOM (Jurnal Riset Komputer),* 9(3), 591-599. http://dx.doi.org/10.30865/jurikom.v9i3.4181

Irawan, I. (2018). Pengembangan Sistem Informasi Akademik Universitas Pahlawan Tuanku Tambusai Riau. *JURNAL TEKNOLOGI DAN OPEN SOURCE,* 1(2), 55–66. https://dx.doi.org/10.36378/jtos.v1i2.21

Jakaria, D. A., dan Dirgahayu, R. T. (2013). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI) 2013*. Yogyakarta: Universitas Islam Indonesia Yogyakarta.

Kholifah K., Putra, R. A., dan Nopriani, F. (2021). Analisis Penilaian Risiko Terhadap Penggunaan Sistem Informasi Akademik Pada Universitas Muhammadiyah Palembang Menggunakan Metode Octave Allegro. *Journal of Computer and Information Systems Ampera*, 2(1), 28–42. https://doi.org/10.51519/journalcisa.v2i1.58

Kuntari, N. L., Chrisnanto, Y. H., dan Hadiana, A. I. (2018). Manajemen Risiko Sistem Informasi di Universitas Jenderal Achmad Yani Menggunakan Metode Octave Allegro. T*eknologi Informasi dan Geospasial di Era Masyarakat Ekonomi ASEAN*. Vol. 1, 551-559. Bogor: Teknik Informatika Universitas Ibn Khaldun Bogor.

Kuo, C. (2007). *Safety Management and Its Maritime Application*. Nautical Institute.

Matondang, N., Isnainiyah, I. N., dan Muliawati, A. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi),* 2(1), 282–287. https://doi.org/10.29207/resti.v2i1.96

McDermott, R. E., Mikulak, R. J., dan Beauregard, M. R. (2009). *The Basics of FMEA 2nd Edition*. New York: Taylor and Francis Group.

Nugraha, U. (2016). Manajemen Risiko Sistem Informasi pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST SP 800-30. Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016), 121-126. Bandung: Universitas Pasundan.

Nurochman, A. (2014). Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan Universitas Gadjah Mada Yogyakarta). *Berkala Ilmu Perpustakaan dan Informasi,* 10(2), 1–13. https://doi.org/10.22146/bip.8830

Purwanto, R. (2017). Penerapan Sistem Informasi Akademik (SIA) sebagai Upaya Peningkatan Efektifitas dan Efisiensi Pengelolaan Akademik Sekolah. *JTT (Jurnal Teknologi Terapan)*, 3(2), 24-31. https://doi.org/10.31884/jtt.v3i2.58

Putri, A. H., dan Kusumawati, Y. (2017). Strategi Mitigasi Risiko Aset Kritis Teknologi Informasi Menggunakan Metode Octave Dan FMEA. *Techno.Com,* 16(4), 367–377. https://doi.org/10.33633/tc.v16i4.1484

Ramdhany, T., dan Krisdiawan, R. A. (2018). Analisis Risiko Sistem Informasi Penjualan Berbasis ISO 31000 - Risk Management Di PT. Remaja Rosdakarya. *Jurnal Teknologi & Manajemen Informatika,* 3(1), 1–7. https://doi.org/10.25134/jejaring.v3i1.1220

Sandhyavitri, A., dan Saputra, N. (2013). Analisis Risiko Jalan Tol Tahap Pra Konstruksi (Studi Kasus Jalan Tol Pekan Baru-Dumai). *Jurnal Teknik Sipil,* 9(1), 1–19. http://dx.doi.org/10.28932/jts.v9i1.1366

Setyadi, G., dan Kusumawati, Y. (2016). Mitigasi Risiko Aset Dan Komponen Teknologi Informasi Berdasarkan Kerangka Kerja OCTAVE Dan FMEA Pada Universitas Dian Nuswantoro. *JOINS (Journal of Information System),* 1(1), 1–10. https://doi.org/10.33633/joins.v1i01.1167

Supradono, B. (2009). Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). *Media Elektrika*, 2(1), 4–8. https://doi.org/10.26714/me.v2i1.480

Wahyuari W., dan Sidik, S. (2023). Manajemen Risiko Sistem Informasi Ujian Secara Daring Di Sekolah Tinggi Manajemen Asuransi Trisakti. *Jurnal Green Growth dan Manajemen Lingkungan,* 12(1), 84–97. https://doi.org/10.21009/10.21009/jgg.v12i1.06

Wijayanti, R. R. (2018). Implementasi OCTAVE-S dan Standar Pengendalian ISO 27001:2013 pada Manajemen Risiko Sistem Informasi Perguruan Tinggi. *PETIR*, 11(2), 221–233. https://doi.org/10.33322/petir.v11i2.351