JORAPI : Journal of Research and Publication Innovation
Vol. 2, No. 2, April 2024 **ISSN 2985-4768**
Halaman : 1479-1491

ANALISIS MANAJEMEN RISIKO PADA SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK OCTAVE ALLEGRO

Khoirun Nadiya[1], Nila Choirun Nisa[2], and Salsabila Annafi'u Nur Aini[3] Adinda Umay Putri Sutan Jandi[4]

[1]Sistem Informasi, Universitas Islam Negeri Sunan Ampel, Surabaya, Jl. Ahmad Yani No.117, Wonocolo-Surabaya, Indonesia, 60237
e-mail: [1]khoirunnadiya@gmail.com

[2,3,4]Sistem Informasi, Universitas Islam Negeri Sunan Ampel, Surabaya, Jl. Ahmad Yani No.117, Wonocolo-Surabaya, Indonesia, 60237

e-mail: [2]nilachoirunnisa056@gmail.com, [3]salsabilanur79@gmail.com, [4]adinda.ummay05gmail.com

Abstract

Academic Information Systems can help universities in academic management. The Academic Information System is managed by the data center and information technology in which there are IT stakeholders. If universities cannot identify the source of threats, then the implementation of academic information systems can pose a risk. Therefore, risk management is needed to detect risk threats as early as possible so that risk prevention or mitigation can be carried out. Risk management is a structured action used for risk identification, assessment, and prevention. This research uses Octave Allegro which has 8 steps, including setting risk measurement criteria, profiling information assets, identifying information asset containers, identifying problem areas, identifying threat scenarios, identifying risks, analyzing risks, and selecting mitigation approaches. The Octave Allegro method is used to determine data security threats. The purpose of this research is to conduct a risk analysis of academic information systems which results in a risk assessment and recommendations related to things that need to be prevented or mitigated. The risk assessment is focused on predetermined areas of concern.

Abstrak

Sistem Informasi Akademik dapat membantu perguruan tinggi dalam pengelolaan akademik. Sistem Informasi Akademik dikelola oleh pusat data dan teknologi informasi yang didalamnya terdapat *stakeholder* IT. Jika perguruan tinggi tidak dapat mengidentifikasi sumber ancaman, maka penerapan sistem informasi akademik dapat menimbulkan risiko. Oleh karena itu diperlukan manajemen risiko untuk mendeteksi ancaman risiko sedini mungkin sehingga dapat dilakukan pencegahan atau mitigasi risiko. Manajemen risiko adalah tindakan terstruktur yang digunakan untuk identifikasi, penilaian, serta pencegahan risiko. Penelitian ini menggunakan Octave Allegro yang terdapat 8 langkah, diantaranya menetapkan kriteria pengukuran risiko, membuat profil aset informasi, mengidentifikasi kontainer aset informasi, mengidentifikasi area masalah, mengidentifikasi skenario ancaman, mengidentifikasi risiko, menganalisis risiko, serta memilih pendekatan mitigasi. Metode Octave Allegro digunakan untuk menentukan ancaman keamanan data. Tujuan penelitian ini adalah untuk melakukan analisis risiko sistem informasi akademik yang hasilnya berupa penilaian risiko dan rekomendasi terkait hal-hal yang perlu

dilakukan pencegahan atau mitigasi. Penilaian risiko difokuskan pada *area of concern* yang telah ditentukan sebelumnya.

Kata kunci: *Manajemen Risiko; Sistem Informasi Akademik; Octave Allegro*

1. PENDAHULUAN

Evolusi Teknologi Informasi, mendorong keinginan individu untuk memperoleh dan mengelola informasi semakin meningkat, hal ini mencerminkan bahwa perkembangan teknologi telah mempercepat dan menyederhanakan proses akses informasi, sekaligus menciptakan tuntutan yang lebih besar dari masyarakat untuk memiliki kontrol penuh terhadap informasi tersebut. Kemudahan teknologi informasi di lingkungan perguruan tinggi telah menghadirkan kemudahan signifikan, terutama dalam hal akses cepat dan ekonomis terhadap informasi melalui Sistem Informasi digital. Sistem Informasi akademik merupakan bagian yang penting dari operasional perguruan tinggi modern. Sistem ini tidak hanya mencakup manajemen data mahasiswa, dosen, dan program studi, tetapi juga menyimpan informasi penting terkait dengan jadwal kuliah, nilai, dan aspek administratif lainnya. Keamanan Sistem Informasi akademik menjadi kunci untuk mendukung efisiensi dan efektivitas operasional perguruan tinggi [1].

Sistem Informasi Akademik beroperasi dalam lingkungan yang kompleks dan terus berkembang. Dengan adanya berbagai jenis data sensitif, seperti informasi pribadi mahasiswa dan rekam jejak akademik, Sistem Informasi Akademik rentan terhadap berbagai ancaman keamanan, termasuk serangan siber, kehilangan data, atau gangguan operasional. Karena perkembangan teknologi informasi yang cepat menimbulkan tantangan tersendiri. Perguruan tinggi cenderung mengadopsi teknologi baru untuk meningkatkan layanan efisien, tetapi seiring dengan adanya sistem tersebut risiko keamanan juga semakin kompleks dan meningkat. Dalam menghadapi kompleksitas dan kerentanan tersebut, diperlukan manajemen risiko. Tujuan manajemen risiko teknologi informasi adalah untuk mengurangi dan mengelola dampak kerusakan, sehingga organisasi dapat menghindari potensi kerugian finansial, penurunan reputasi, gangguan operasional, kegagalan evaluasi aset, dan penundaan pengambilan keputusan.

Framework seperti Octave Allegro menyediakan landasan yang kokoh untuk menganalisis, menilai, dan mengelola risiko keamanan informasi, khususnya dalam konteks Sistem Informasi Akademik. Octave merupakan sebuah metode untuk manajemen dan analisis risiko teknologi informasi. Octave dibangun untuk memungkinkan penilaian dan perancangan keamanan sistem informasi berbasis risiko, itu adalah alat, metode, dan pendekatan. Dengan menggunakan octave allegro, perguruan tinggi dapat memperoleh wawasan yang lebih tajam tentang risiko pada sistem informasi akademik[2]. Dengan cara ini perguruan tinggi dapat memproteksi dengan lebih baik aset informasi yang kritis dan merencanakan langkah-langkah keamanan yang sesuai.

2. PENELITIAN YANG TERKAIT

Pada penelitian terkait di uraikan definisi terkait dengan risiko, manajemen risiko, sistem informasi akademik, serta metode OCTAVE Allegro.

2.1 Risiko

Risiko dapat diartikan sebagai konsekuensi negatif yang timbul dari kerentanan, dimana risiko merupakan konsekuensi yang tidak diinginkan dari suatu peristiwa atau kejadian tertentu yang dapat menyebabkan kerugian dan memiliki konsekuensi yang tidak dapat diprediksi [3]. Sarno mendefinisikan risiko sebagai suatu kesempatan atau kemungkinan yang dapat mempengaruhi suatu tujuan, tetapi dapat menyebabkan kerugian jika risiko tidak dikelola dengan baik. Risiko melibatkan tiga tahapan proses utama, diantaranya adalah penilaian risiko, mitigasi risiko, dan evaluasi [4].

Adanya risiko dapat menyebabkan aktivitas sistem melemah dan sistem tidak beroperasi secara optimal. Risiko dapat dibedakan menjadi risiko internal dan risiko eksternal. isiko internal dapat berasal dari kegagalan sistem dan jaringan (network), kerusakan hardware dan software, kehilangan data, dan kemungkinan virus. Di sisi lain, risiko eksternal seperti gangguan alam seperti petir, hujan, banjir, dan angin kencang dapat menyebabkan kerusakan infrastruktur TI dan mengganggu operasi normal [5].

Risiko memang tidak dapat dihilangkan sepenuhnya tetapi dapat dikelola. Oleh karena itu, memiliki manajemen risiko sangat penting guna untuk mempersiapkan perusahaan atau organisasi dalam menghadapi perubahan di lingkungan, pasar, atau regulasi yang dapat mempengaruhi operasional mereka. Selain itu, manajemen risiko juga berperan dalam menciptakan perbaikan berkelanjutan dan membantu mengurangi dampak negatif, seperti kerugian akibat dari adanya potensi risiko yang mungkin terjadi di perusahaan tersebut.

2.2 Manajemen Risiko

Manajemen risiko merupakan tahap atau tindakan yang terstruktur untuk melakukan identifikasi, penilaian, dan melakukan sebuah tindakan guna mengantisipasi risiko agar dapat diterima oleh organisasi [1].

Identifikasi risiko, penilaian risiko, dan pengendalian risiko adalah tiga bagian dari manajemen risiko. Kesuksesan manajemen risiko bergantung pada kemampuan (kapabilitas), cara pandang (persepsi), dan niat (intensi) individu yang terlibat dalam proses pelaksanaannya [6].

Analisis manajemen risiko adalah prosedur yang dilakukan di tingkat pelaksana manajemen, dimana hal ini meliputi melakukan analisis sistematis terhadap kerugian yang dialami oleh sebuah perusahaan dan akibat yang ditimbulkan dari adanya risiko tersebut, serta mengidentifikasi cara pengendalian yang sesuai untuk mengatasi potensi kerugian di instansi tersebut [7].

2.3 Sistem Informasi Akademik

Sistem informasi merupakan gabungan elemen atau individu yang terhubung satu sama lain dan terintegrasi untuk memproses, menyimpan, serta mendistribusikan informasi [8]. Sistem Informasi Akademik merupakan suatu sistem yang dimaksudkan untuk memenuhi persyaratan pendidikan menggunakan teknologi komputer dengan melibatkan perangkat keras (*hardware*) maupun perangkat lunak (*software*) [1]. Keberadaan Sistem Informasi Akademik mempermudah semua proses kegiatan akademik dapat dilakukan secara efisien sehingga akan berjalan dengan baik dan lancar.

Data yang dihasilkan oleh Sistem Informasi Akademik bisa dijadikan sumber informasi yang berharga dalam untuk mengelola manajemen institusi pendidikan tinggi dan mendukung pengambilan keputusan oleh para pemimpin di lingkungan perguruan tinggi [1]. Banyak fungsi utama dalam Sistem Informasi Akademik seperti menyimpan informasi data pribadi mahasiswa, membantu dalam pembuatan dan pengelolaan jadwal perkuliahan, mencatat nilai mahasiswa serta menyusun transkrip, menyediakan laporan analisis terkait dengan kinerja akademik mahasiswa, serta memudahkan para dosen dan mahasiswa untuk melakukan komunikasi.

2.4 OCTAVE Allegro

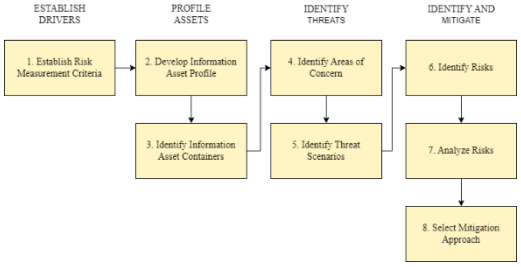
OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) yaitu sebuah metodologi yang berfungsi guna mengidentifikasi dan menilai ancaman terhadap keamanan data. (Ikhsan & Jarti, 2018). Penilaian risiko dalam OCTAVE dilakukan berdasarkan tiga prinsip utama administrasi keamanan yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), *availability* (ketersediaan). Metode Octave memiliki tiga variasi, yaitu OCTAVE, OCTAVE-S, dan OCTAVE Allegro. Meskipun ketiganya tidak saling melengkapi dan menggantikan, masing-masing metode dirancang untuk memenuhi kebutuhan khusus pengguna OCTAVE yang ingin melakukan penilaian risiko [3].

OCTAVE Allegro merupakan metode OCTAVE generasi terbaru yang berfungsi sebagai panduan penilaian risiko yang lebih menekankan pada keamanan aset dan data pendukung informasi [9]. Terutama untuk organisasi yang belum memiliki manajemen risiko yang cukup untuk sistem informasi, metode ini telah terbukti mampu memberikan penilaian risiko yang efektif dengan sedikit investasi dan waktu [10]. Fokus utama OCTAVE Allegro terletak pada aset informasi yang mencakup cara penggunaan, penyimpanan, pengangkutan, dan pemrosesan aset, serta dampaknya jika terkena ancaman, kerentanan, ataupun gangguan [3].

3. METODE PENELITIAN

Metode penelitian dilakukan dengan dua tahapan, yaitu tahap perencanaan dan tahap pengumpulan data. Tahap awal adalah perencanaan, yang dilakukan berdasarkan masalah yang telah ditetapkan. Dalam tahap ini studi pustaka dilakukan untuk menentukan studi kasus dan permasalahan yang akan dilakukan penelitian. Kemudian dari permasalahan tersebut akan dicari solusi sesuai dengan *framework* OCTAVE Allegro [11].

Sedangkan tahap pengumpulan data dilakukan guna memperoleh data dan informasi terkait dengan topik pembahasan dengan cara studi pustaka atau *literature review* dari berbagai sumber referensi berupa jurnal *online* dan sumber lainnya. Pengumpulan data ini berfungsi untuk untuk mengidentifikasi masalah, mendapatkan informasi tentang landasan teori yang diperlukan, menentukan manfaat dan tujuan dari masalah tersebut, dan menentukan batasan penelitian. Dari data yang telah diperoleh akan dilakukan implementasi dengan metode penilaian risiko sesuai tahapan yang terdapat pada *framework* OCTAVE Allegro [12].



Gambar 1. *Tahapan Metode Octave*

Gambar 1 menunjukkan 4 tahapan dan 8 aktivitas. Tahapan yang pertama adalah membangun *drivers*, perusahaan membuat standar pengukuran risiko untuk

melakukan evaluasi dampak risiko pada penggerak organisasi. Standar ini berhubungan dengan semua hal yang membuat organisasi bergerak (pembawa organisasi). Tahap kedua adalah membuat profil aset yang berfokus pada identifikasi aset untuk penilaian risiko, serta identifikasi aset kontainer. Dalam hal ini Kontener adalah istilah yang mengacu pada media yang digunakan untuk menyimpan, mengirimkan, dan memproses aset data. Tahap ketiga yaitu identifikasi ancaman, Identifikasi ancaman adalah fase di mana ancaman diidentifikasi dan didokumentasikan. Ancaman ini dapat berupa pernyataan deskriptif (*area of concern*) atau gambaran secara terstruktur (*threat scenario*) [12]. Tahap terakhir adalah identifikasi dan mitigasi risiko yang dilakukan berdasarkan pada informasi ancaman serta merumuskan rencana untuk mitigasinya [13].

4. HASIL DAN PEMBAHASAN

Struktur OCTAVE Allegro digunakan untuk mengumpulkan data dan informasi tentang manajemen risiko sistem informasi. Terdapat beberapa fase utama, diantaranya adalah melakukan identifikasi risiko, melakukan penilaian risiko, serta mengembangkan strategi perlindungan keamanan pada manajemen sistem informasi akademik [4].

4.1 Identifikasi Risiko

Tujuan dari tahap identifikasi risiko adalah untuk mendapatkan pemahaman tentang berbagai risiko yang mungkin terjadi. Setelah melakukan studi literatur, tahap yang dilakukan dengan mengumpulkan informasi guna mengetahui jenis-jenis risiko yang mungkin timbul dalam operasional bisnis instansi. Dalam tahap ini telah ditentukan empat konteks yang menjadi batasan parameter internal dan eksternal untuk mempertimbangkan sumber risiko, yaitu alam atau lingkungan, manusia, sistem, serta infrastruktur.

Tabel 1. *Daftar Risiko*

Kategori Risiko	**Risiko**	**Penyebab**	**Dampak**
Alam atau lingkungan	Petir	Bencana alam	Koneksi jaringan terganggu
	Kebakaran	Korsleting listrik	Kerugian bagi perusahaan
Manusia	*Human Error*	Kurangnya pelatihan karyawan baru	Kerugian bagi perusahaan
Sistem dan Insfrastruktur	Server down	Listrik padam	Sistem tidak dapat diakses
	Data corrupt	Virus	Data tidak dapat diakses/ditemukan
	Koneksi jaringan tidak stabil	Gangguan pada provider Listrik padam	Sistem tidak dapat diakses
	Gagal update	Server down, listrik padam	Data tidak dapat disimpan
	Kerusakan Hardware	Arus listrik tidak stabil	Kerugian terhadap material perusahaan
	Overheat	Cuaca Panas	Perangkat panas, sistem tidak dapat dioperasikan
	Listrik Padan	Perbaikan dari PLN	Tidak bisa melakukan aktivitas pada sistem

4.2 Penilaian Risiko

Tahap awal yang perlu dilakukan sebelum melaksanakan penilaian risiko adalah melakukan pengumpulan data dari orang-orang yang bertanggung jawab atas pengelolaan di divisi IT, meliputi Kepala IT, Staff IT, dan Admin SIAKAD. Penilaian risiko yang dilakukan menggunakan *framework* OCTAVE Allegro perlu melalui delapan tahapan, diantaranya sebagai berikut.

1. Langkah 1 - Menetapkan Kriteria Pengukuran Risiko

Pada langkah awal ini, perlu untuk mengidentifikasi dampak area dan memberikan nilai skala prioritas untuk dampak area tersebut. Dalam

proses menentukan *impact area* dapat dengan mempertimbangkan misi serta tujuan bisnis pada organisasi yang bersangkutan. Adapun prioritas *impact area* yang telah ditentukan meliputi keamanan dan kesehatan, produktivitas, reputasi dan kepercayaan pelanggan, finansial, serta denda dan penalti. Pada tabel 2 berisi hasil penentuan *impact area* dan tabel 3 merupakan skala prioritas *impact area*.

Tabel 2. *Impact Area*

Impact Area	Low	Medium	High
Reputasi	Reputasi sedikit terpengaruh, sehingga diperlukan usaha kecil untuk perbaikannya.	Reputasi terkena dampak buruk, sehingga perlu melakukan usaha perbaikan dan biaya untuk meningkatkannya.	Penurunan reputasi yang besar atau telah rusak yang menyebabkan hampir tidak dapat diperbaiki.
Kehilangan Kepercayaan Pelanggan	Terjadi penurunan pelanggan kurang dari 2% karena hilangnya kepercayaan.	Penurunan pelanggan antara 2% hingga 10% yang disebabkan karena hilangnya kepercayaan.	Pengurangan pelanggan lebih dari 10% yang diakibatkan hilangnya kepercayaan.
Keamanan	Terjadi insiden keamanan yang berdampak ringan yaitu gangguan server sementara sehingga pengguna tidak dapat mengakses sistem	Terjadi insiden keamanan yang cukup serius yaitu kebocoran data pengguna, sehingga perlu dilakukan tindakan untuk meminimalisir dampak yang	Terjadi insiden keamanan yang serius yang mengakibatkan sistem tidak dapat diakses, kehilangan data pengguna, dan berdampak finansial.
		mungkin terjadi.	
Kesehatan	Pengguna merasa tidak nyaman ataupun kebingungan karena tidak dapat mengakses sistem,	Pengguna mulai merasa khawatir terhadap keamanan data pribadi mereka yang rentan mengalami kebocoran data.	Pengguna merasa panik karena sudah tidak dapat mengakses sistem dan khawatir terhadap kebocoran data pribadi miliknya.
Produktivitas	Terhambatnya produktivitas pengguna saat ingin mengakses dan menggunakan sistem tersebut ataupun memperoleh informasi.	Memiliki pengaruh yang cukup signifikan pada lambatnya produktivitas dan kegiatan operasional yang akan dilakukan pengguna.	Berpotensi menyebabkan kerugian serius terhadap produktivitas, kegiatan operasional, dan reputasi sistem karena tidak dapat digunakan.
Finansial	Terjadi gangguan sementara pada sistem pembayaran, sehingga pengguna mengalami sedikit kendala saat ingin melakukan pembayaran.	Gangguan pada sistem pembayaran dapat berpotensi menyebabkan kerugian pendapatan pada institusi tersebut.	Berpotensi mengalami kerugian finansial yang signifikan dan dapat berpengaruh pada pengelolaan dana dan investasi menjadi terhambat.

Denda dan Penalti	Terjadi pelanggaran ringan sehingga berpotensi terkena denda kecil yang masih dapat ditanggung oleh institusi.	Berpotensi terkena denda cukup besar yang disebabkan salah satunya karena pelanggaran kebijakan keamanan data pengguna.	Terjadi pelanggaran yang serius salah satunya terhadap data pengguna, sehingga berpotensi terkena denda sangat besar yang merugikan dana institusi dalam jangka panjang.

Tabel 3. *Skala Prioritas Impact Area*

Priority	Impact Area
5	Reputasi dan Kepercayaan Pelanggan
4	Keamanan dan Kesehatan
3	Produktivitas
2	Finansial
1	Denda dan Penalti

2. Langkah 2 - Membuat Profil Aset Informasi.

Pada langkah ini, profil aset informasi yang penting bagi organisasi harus diidentifikasi untuk mengurangi risiko terhadap aset informasi yang penting [14].

Tabel 3. *Profil Aset Informasi*

PROFIL ASET INFORMASI KRITIS		
(1) Aset Kritis Aset informasi siapa yang kritis?	**(2) Alasan untuk seleksi** Mengapa aset informasi ini penting bagi organisasi?	**(3) Keterangan** Apa deskripsi yang disepakati aset informasi ini?
Aset informasi Akademik	Karena jika aset data informasi ini bocor atau hilang dapat disalahgunakan karena melibatkan data dan informasi penting yang menjadi pendukung proses utama dalam kegiatan operasional akademik.	Aset informasi ini terdapat data penting mahasiswa, dosen, dan bagian akademik lainnya (seperti data pribadi, KRS, KHS, Transkrip nilai, absensi, data dosen dan bagian akademik lainnya).
(4) Pemilik Siapa yang memiliki aset informasi ini?		
Mahasiswa, Dosen, Staf Admin Database, dan Pusat Data dan Teknologi Informasi (Pemangku kepentingan IT pada perguruan tinggi).		
(5) Persyaratan Keamanan Apa persyaratan keamanan untuk aset informasi ini?		
Menyusun dan menerapkan kebijakan keamanan informasi yang jelas dan dapat dipahami, menggunakan metode otentikasi yang kuat untuk mengonfirmasi identitas pengguna sebelum memberikan akses ke aset informasi sensitif, mengenkripsi data sensitif saat berpindah melalui jaringan atau disimpan di repositori data untuk melindungi data dari akses yang tidak sah, melindungi fisik dari server dari sistem penyimpanan yang mengandung aset informasi, menerapkan solusi pemulihan bencana untuk memastikan kesediaan kembali sistem dan data setelah insiden, memberikan pelatihan keamanan informasi pada semua pengguna.		

3. Langkah 3 - Mengidentifikasi Kontainer Aset Informasi

Kontainer adalah tempat aset disimpan, dikirim, atau diproses. Dalam konteks keamanan, Kontener ini dapat berfungsi sebagai sumber kerentanan dan ancaman yang dapat membahayakan aset informasi. Namun sebaliknya, kontainer juga dapat menjadi lokasi di mana kontrol keamanan dilakukan, terutama di mana aset informasi dalam berbagai jenis seperti perangkat keras, perangkat lunak, atau sistem tersimpan [15]. Terdapat tiga poin utama dalam keamanan dan konsep kontainer, poin tersebut meliputi aspek teknis, manusia, dan fisik.

Tabel 4. *Kontainer Aset Informasi*

PETA LINGKUNGAN RISIKO ASET INFORMASI	
Internal	
Deskripsi	**Pemilik**
1. Module: Database layanan Sistem Informasi Akademik didalam server yang digunakan oleh Kepala IT, Staff IT, admin, mahasiswa dan dosen dalam menggunakan layanan.	Pusat Data dan Teknologi Informasi (Pemangku kepentingan IT pada perguruan tinggi)
2. Server: wadah untuk penyimpanan aplikasi dan database dengan menggunakan jaringan internet	
3. Jaringan Internet Internal: LAN	
4. Komputer: perangkat komputer server	
5. Sistem Operasi Server: Windows server	
6. Aplikasi: Sistem Informasi Akademik (SIAKAD)	
Eksternal	
Deskripsi	**Pemilik**
Jaringan Internet: Menggunakan vendor pihak ketiga	Indihome

4. Langkah 4 - Mengidentifikasi Area Masalah

Mengidentifikasi area masalah dapat dilakukan dengan meninjau setiap wadah atau kontainer untuk mengidentifikasi area yang perlu diperhatikan, dan kemudian menyimpan catatan untuk setiap area yang telah diidentifikasi [16].

Tabel 5. *Area of Concern*

No.	***Area of Concern***
1.	*Database* menemukan kesalahan atau *error* selama *maintenance*.
2.	*Server down* yang menyebabkan semua layanan tidak dapat diakses oleh semua pihak.
3.	Ruangan server yang mudah diakses menyebabkan pihak yang tidak berwenang dapat mengakses server.
4.	Kerusakan pada perangkat komputer *hardware*.
5.	Kebocoran dan penyebaran hak akses yang dapat menyebabkan penyelewengan.

5. Langkah 5 - Mengidentifikasi Skenario Ancaman

Pada langkah ini dilakukan identifikasi dan pandangan terkait skenario ancaman dari tiap *area of concern* yang telah ditentukan untuk memperjelas detail properti dari sebuah ancaman. Detail properti dari sebuah ancaman antara lain *actor, means, motives, outcome,* dan *security*).

Tabel 6. *Identifikasi Skenario*

1	***Area of Concern***	***Threat of Properties***	
	Database menemukan kesalahan atau *error* selama *maintenance*.	***Actor***	Staf Database Admin
		Means	Data yang ditampilkan dapat mengalami kesalahan atau bahkan tidak valid.
		Motives	Kesalahan sistem yang dapat terjadi tanpa sengaja ataupun dengan kesengajaan.
		Outcome	• Disclosure • Destruction • Modification
		Security Requirements	Melakukan perbaikan secara berkala untuk mengurangi resiko kerusakan.

	Kemungkinan/ Probabilitas	*High*	
	Area of Concern	***Threat of Properties***	
2	*Server down* yang menyebabkan semua layanan tidak dapat diakses oleh semua pihak.	***Actor***	*Stakeholder* IT
		Means	Server tidak bisa diakses karena penuh atau terdapat *bug*.
		Motives	Tidak Disengaja
		Outcome	• Interruption • Modification
		Security Requirements	Melakukan pengecekan server secara berkala.
	Kemungkinan/ Probabilitas	*High*	
3	***Area of Concern***	***Threat of Properties***	
	Ruangan server yang mudah diakses menyebabkan pihak yang tidak berwenang dapat mengakses server.	***Actor***	Tidak Diketahui
		Means	• Destruction • Disclosure • Interruption
		Motives	Disengaja
		Outcome	• Interruption
			• Penyalahgunaan data
		Security Requirements	Memperkuat keamanan sistem dengan membatasi pengguna hanya untuk orang yang berwenang.
	Kemungkinan/ Probabilitas	*Medium*	
4	***Area of Concern***	***Threat of Properties***	
	Kerusakan pada perangkat komputer *hardware*.	***Actor***	Tidak Diketahui
		Means	Perangkat komputer mengalami kerusakan pada bagian tertentu.
		Motives	Secara sengaja maupun tidak disengaja.
		Outcome	• Interruption • Destruction
		Security Requirements	Melakukan *service* dan memastikan *hardware* berada ditempat yang aman.
	Kemungkinan/ Probabilitas	*Medium*	
5	***Area of Concern***	***Threat of Properties***	
		Actor	Tidak Diketahui

	Kebocoran dan penyebaran hak akses yang dapat menyebabkan penyelewengan.	***Means***	Data hak akses pengguna bocor kepada orang yang tidak berwenang.
		Motives	Secara sengaja atau tidak sengaja memberitahukan informasi hak akses seperti *username* dan *password*.
		Outcome	• Disclosure • Modification • Interruption
		Security Requirements	Membuat kebijakan untuk mengelola akses masuk pribadi pengguna ke sistem serta melakukan reset *password* secara berkala.
	Kemungkinan/ Probabilitas	*High*	

6. Langkah 6 - Mengidentifikasi Risiko

Langkah ini dilakukan untuk mengevaluasi dampak dari skenario ancaman. Setiap skenario yang telah dibuat harus mempertimbangkan konsekuensi dan efek yang dapat ditimbulkannya.

Tabel 7. *Identifikasi Risiko*

Impact Areas	***Priority***	***Low* (1)**	***Medium* (2)**	***High* (3)**
Reputasi dan Kepercayaan Pelanggan	5	5	10	15
Keamanan dan Kesehatan	4	4	8	12
Produktivitas	3	3	6	9
Finansial	2	2	4	6
Denda dan Penalti	1	1	2	3

7. Langkah 7 - Menganalisis Risiko

Analisis risiko dilakukan pada setiap *area of concern*, hal pertama yang harus dilakukan adalah meneliti standar pengukuran risiko, kemudian menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko untuk menentukan mitigasi terbaik [17].

Tabel 8. *Analisis Risiko*

Area of Concern	***Risk***			
Database menemukan kesalahan atau *error* selama *maintenance*.	***Consequences***	Server tidak dapat diakses, sehingga tidak dapat menyimpan data.		
	Severity	***Impact Area***	***value***	***Score***
		Reputasi dan Kepercayaan Pelanggan	High	15
		Keamanan dan Kesehatan	Medium	8
		Produktivitas	High	9
		Finansial	Low	2
		Denda dan Penalti	Low	1
		Relative Risk Score		35

Area of Concern	***Risk***			
Server down yang menyebabkan semua layanan tidak dapat diakses oleh semua pihak.	***Consequences***	Pengguna tidak dapat mengakses layanan yang disediakan atau dapat diakses tetapi membutuhkan waktu yang lama.		
	Severity	***Impact Area***	***value***	***Score***
		Reputasi dan Kepercayaan Pelanggan	High	15
		Keamanan dan Kesehatan	Medium	8
		Produktivitas	High	9
		Finansial	Low	2
		Denda dan Penalti	Low	1
		Relative Risk Score		35

Area of Concern	***Risk***			
Ruangan server yang mudah diakses menyebabkan pihak yang tidak berwenang dapat mengakses server.	***Consequences***	Server dapat diakses oleh orang yang tidak bertanggungjawab dan data dapat disalahgunakan.		
	Severity	***Impact Area***	***value***	***Score***
		Reputasi dan Kepercayaan Pelanggan	Med	10
		Keamanan dan Kesehatan	High	12
		Produktivitas	Low	3
		Finansial	Low	2
		Denda dan Penalti	Low	1
		Relative Risk Score		28

Area of Concern	***Risk***			
Kerusakan pada perangkat komputer *hardware*.	***Consequences***	Stakeholder harus menyediakan perangkat baru.		
	Severity	***Impact Area***	***value***	***Score***
		Reputasi dan Kepercayaan Pelanggan	Low	5
		Keamanan dan Kesehatan	Medium	8
		Produktivitas	High	9
		Finansial	High	6
		Denda dan Penalti	Low	1
		Relative Risk Score		29

Area of Concern	***Risk***			
Kebocoran dan penyebaran hak akses yang dapat menyebabkan penyelewengan.	***Consequences***	Penyalahgunaan data dan informasi terkait pengguna.		
	Severity	***Impact Area***	***value***	***Score***
		Reputasi dan Kepercayaan Pelanggan	High	15
		Keamanan dan Kesehatan	High	12
		Produktivitas	Low	3
		Finansial	Medium	4
		Denda dan Penalti	Low	1
		Relative Risk Score		35

8. Langkah 8 - Memilih Pendekatan Mitigasi

Pada langkah ini hal yang harus dilakukan pertama yaitu mengelompokkan risiko dan memilih pendekatan mitigasi sesuai dengan nilai identifikasi risiko [18].

Tabel 9. *Pendekatan Mitigasi*

RISK SCORE		
30 TO 45	**16 TO 29**	**0 TO 15**
POOL 1	POOL 2	POOL 3
High	Medium	Low
Mitigate	Mitigate or Deafer	Accept

Tabel 10. *Penentuan Pendekatan Mitigasi*

No	**Area of concern**	**Relative Risk Score**	**Probabilitas**	**POOL**	**Pendekatan Mitigasi**
1.	*Database* menemukan kesalahan atau *error* selama *maintenance*.	35	*High*	POOL 1	*Mitigate*
2.	*Server down* yang menyebabkan semua layanan tidak dapat diakses oleh semua pihak.	35	*High*	POOL 1	*Mitigate*
3.	Ruangan server yang mudah diakses menyebabkan pihak yang tidak berwenang dapat mengakses server.	28	*Medium*	POOL 2	*Mitigate or Deafer*
4.	Kerusakan pada perangkat komputer *hardware*.	29	*Medium*	POOL 2	*Mitigate or Deafer*
5.	Kebocoran dan	35	*High*	POOL 1	*Mitigate*

	penyebaran hak akses yang dapat menyebabkan penyelewengan.				

5. KESIMPULAN

Manajemen risiko sangat penting dilakukan untuk mengantisipasi atau mencegah ancaman risiko yang dapat terjadi dalam Sistem Informasi Akademik. Untuk melakukan penilaian risiko diperlukan metode yang efektif dalam klasifikasi risiko. Untuk penelitian ini, digunakan metode penilaian risiko Octave Allegro. Octave Allegro terdiri dari delapan langkah utama yaitu, menetapkan standar pengukuran risiko, membuat profil informasi aset, menemukan wadah informasi aset, menemukan area perhatian, menemukan skenario ancaman, menemukan risiko, menganalisis risiko, dan memilih strategi pengurangan atau mitigasi.

Dalam penelitian ini ditentukan 5 *impact areas* diantaranya yaitu reputasi dan kepercayaan pengguna, keamanan dan kesehatan, produktivitas, finansial, serta denda dan penalti, serta berfokus pada 5 *areas of concern*. Dari *areas of concern* yang telah ditentukan menghasilkan 3 *area* harus dilakukan mitigasi dan 2 harus di mitigasi atau harus diantisipasi. Manajemen risiko keamanan informasi yang memiliki probabilitas tinggi perlu dilakukan dan dipantau secara ketat. Hasil penilaian risiko tersebut dapat dijadikan panduan untuk membuat perencanaan strategis guna menjaga aset informasi dengan tepat.

DAFTAR PUSTAKA

[1] E. Ardius and D. Syamsuar, "Assessment Risk Terhadap Penggunaan Sistem Informasi Akademik Universitas Ea Menggunakan Metode ISO 27001," 2023.

[2] N. Budarsa, G. Indrawan, and A. Gunadi, "Analisis Risiko Keamanan Informasi Menggunakan Metode Octave Allegro Dan Analytical Hirarchy Process Pada Data Center Pemerintah Kabupaten Buleleng," *Jurnal Ilmu Komputer Indonesia (JIK)*, vol. 7, no. 1, 2022.

[3] H. Ikhsan and N. Jarti, "Analisis Risiko Keamanan Teknologi Informasi Menggunakan Octave Allegro," *Responsive Teknik Informatika*, vol. 2, no. 1, pp. 31–41, 2018.

[4] D. R. Nurfadilah, W. Hayuhardhika, N. Putra, and A. Rachmadi, "Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001:2013 (Studi Kasus: Aplikasi E-Kinerja)," *Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 4, no. 9, pp. 3014–3020, 2020, [Online]. Available: http://j-ptiik.ub.ac.id

[5] Y. Erlika *et al.*, "Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000," *Informatika Global*, vol. 11, no. 01, pp. 55–62, 2020.

[6] R. Fahlepi *et al.*, "Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000," 2023.

[7] F. Harimurti, "Manajemen Risiko, Fungsi dan Mekanismenya," *Ekonomi dan Kewirausahaan*, vol. 6, no. 1, pp. 105–112, 2006.

[8] H. T. Sihotang, "Sistem Informasi Pengadendaan Surat Berbasis Web Pada Pengadilan Tinggi Medan," *Journal Of Informatic Pelita Nusantara*, vol. 3, no. 1, pp. 6–9, 2018.

[9] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. 2007. [Online]. Available: http://www.sei.cmu.edu/publications/pubweb.html

[10] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan

System Integrator Menggunakan Metode Octave Allegro," *Jurnal Teknologi dan Informasi (JATI)*, vol. 12, no. 27, p. 12, 2022, doi: 10.34010/jati.v12i2.

[11] I. P. Ramayasa, "Penerapan Framework Itil V3 Dalam Analisis Tata Kelola Sistem Informasi Layanan Akademik Domain Service Transition," *Teknologi Informasi dan Komputer*, vol. 06, no. 02, pp. 134–141, 2020.

[12] P. N. Emmanuel and R. Maulany, "Penilaian Risiko Sistem Informasi Menggunakan Metode OCTAVE Allegro pada Indonesia Publishing House," *KREA-TIF: TEKNIK INFORMATIKA*, vol. 11, no. 1, pp. 37–52, 2023, doi: 10.32832/krea-tif.v11i1.14179.

[13] A. Pakarbudi, D. T. Piay, D. Nurmadewi, and A. Rachman, "Analisa Efektivitas Metode Octave Allegro dan Fmea Dalam Penilaian Risiko Aset Informasi Pada Institusi Pendidikan Tinggi," JURIKOM (Jurnal Riset Komputer), vol. 10, no. 2, p. 488, Apr. 2023, doi: 10.30865/jurikom.v10i2.5950.

[14] R. Wini Astuti, R. A. Putra, and I. S. Putra, "Penilaian Risiko Penggunaan Sistem Informasi Akademik Pada STIQ Al-Lathifiyyah Palembang Dengan Metode Octave Allegro," *Journal of Computer and Information Systems Ampera*, vol. 4, no. 1, pp. 44–54, Jan. 2023, doi: 10.51519/journalcisa.v4i1.337.

[15] R. Diansyah, I. C. Armae, Novalia. Melly, and Nesdi. E. Rozanda, "Identifikasi Risiko Aset Informasi Pada Sistem Informasi Akademik," *FASILKOM (Fakultas Ilmu Komputer)*, vol. 8, no. 1, pp. 289–298, 2019.

[16] D. A. Jakaria, R. T. Dirgahayu, and Hendrik, "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, 2013, pp. 15–2013.

[17] J. Sanjaya, "Analisis Risk Assessment terhadap Perusahaan IT di Bidang Finansial menggunakan OCTAVE Allegro Framework Analisis Risk Assessment Terhadap Perusahaan It Di Bidang Finansial Menggunakan Octave Allegro Framework," Teknologi Informasi dan Komputer, vol. 10, no. 1, pp. 57–67, 2020.

[18] P. Ramjanati, F. K. Wijaya, and M. S. Muarie, "Penilaian Risiko Keamanan Informasi Menggunakan Octave Allegro: Studi Kasus pada Perguruan Tinggi," *Jurnal Sistem Informasi (JUSTIFO)*, vol. 7, no. 1, pp. 10–20, 2021.