PENERAPAN OCTAVE ALLEGRO DALAM MANAJEMEN RISIKO SISTEM INFORMASI PADA UNIVERSITAS ISLAM XYZ

Zahra Nur Fadhila, Ilham
Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Ampel
Jl. Ahmad Yani No.177, Jemur Wonosari, Kec. Wonocolo, Surabaya,Indonesia
zahranuurfadhila@gmail.com

ABSTRAK

Penerapan framework OCTAVE Allegro telah menjadi solusi dalam manajemen risiko keamanan informasi, khususnya untuk sistem informasi akademik Universitas Islam XYZ. Masalah utama yang dihadapi adalah tingginya risiko kebocoran data, penyalahgunaan akses, dan kerentanan sistem informasi yang dapat mengancam efisiensi operasional serta reputasi universitas. Penelitian ini bertujuan untuk mengevaluasi implementasi OCTAVE Allegro dalam mengidentifikasi, menganalisis, dan memitigasi risiko-risiko tersebut. Metodologi penelitian melibatkan dua tahap utama, yaitu studi literatur dan pengumpulan data melalui observasi lapangan. Proses analisis dilakukan dengan mengidentifikasi aset kritis, mengukur risiko, dan menentukan strategi mitigasi berdasarkan prioritas dampak. Temuan menunjukkan bahwa pendekatan ini mampu mengidentifikasi tujuh risiko utama, termasuk kerusakan data, kebocoran informasi pengguna, dan kesalahan dalam pengelolaan data. Framework OCTAVE Allegro memberikan solusi berbasis pengelolaan risiko melalui tindakan mitigasi yang sistematis seperti backup data, kontrol akses fisik, dan verifikasi pengguna. Simpulan dari penelitian ini mengungkapkan bahwa implementasi OCTAVE Allegro terbukti signifikan dalam meningkatkan keamanan informasi dan efisiensi operasional sistem informasi akademik Universitas Islam XYZ. Hasil ini diharapkan dapat menjadi referensi bagi institusi lain dalam mengelola risiko keamanan informasi.

Kata kunci : *Octave Allegro, Manajemen Risiko, Sistem Informasi Akademik, Keamanan Data, Mitigasi Risiko*

1. PENDAHULUAN

Di era digital saat ini, teknologi informasi sangat penting untuk mempertahankan operasional berbagai bisnis. Perkembangan teknologi informasi terus berlanjut seiring dengan meningkatnya kebutuhan akan layanan pendidikan[1]. Kemajuan teknologi informasi dalam lingkungan perguruan tinggi sudah memberikan kemudahan yang besar, khususnya dalam hal kecepatan akses dan efisiensi biaya pada informasi melalui sistem informasi digital[2]. Sistem informasi di Universitas Islam XYZ memegang peranan yang sangat krusial dalam mendukung kegiatan akademik, administrasi, dan operasional universitas. Keberadaan sistem informasi ini memungkinkan pengelolaan data mahasiswa, dosen, keuangan, dan berbagai informasi lainnya secara lebih efisien dan terintegrasi. Menurut Fitz Gerald, sistem informasi terdiri dari serangkaian elemen yang dapat mengumpulkan, mengolah, menyimpan, dan menyalurkan informasi yang berguna untuk membantu proses pengambilan keputusan dalam manajemen sebuah organisasi. Sistem informasi juga berperan dalam membantu level manajerial untuk menganalisis dan memvisualisasikan solusi atas permasalahan yang dihadapi dalam proses bisnis organisasi[3].

Namun, seiring dengan meningkatnya penggunaan teknologi informasi, sebagai lembaga pendidikan tinggi yang mengedepankan nilai-nilai keislaman, Universitas Islam XYZ, juga dihadapkan pada berbagai risiko yang berpotensi mengganggu keamanan informasi. Risiko seperti kebocoran data, serangan siber, atau kerusakan infrastruktur teknologi dapat berdampak buruk terhadap operasional universitas dan reputasi lembaga. Keamanan sistem informasi akademik merupakan faktor utama yang mendukung efisiensi dan efektivitas operasional di perguruan tinggi[4].

Manajemen risiko dalam keamanan sistem informasi menjadi kunci untuk mengidentifikasi, menilai, dan mengurangi risiko-risiko tersebut. Analisis risiko dan pengelolaan risiko merupakan dasar dari manajemen risiko di mana pengendalian risiko berfungsi sebagai keseimbangan antara keamanan, kegunaan, dan biaya[5]. Salah satu framework yang terbukti efektif dalam mengelola risiko keamanan informasi adalah OCTAVE Allegro. Menurut penelitian-penelitian sebelumnya, framework ini terbukti efektif dalam memberikan hasil penilaian risiko yang memadai dapat dicapai dengan alokasi dana dan waktu yang relatif rendah, terutama bagi organisasi yang masih belum menerapkan manajemen risiko yang memadai untuk sistem informasi yang mereka kelola [6]. Kerangka kerja seperti OCTAVE Allegro memberikan dasar yang kuat dalam menganalisis, mengevaluasi, dan mengatur risiko keamanan informasi, terutama dalam ranah Sistem Informasi Akademik [2]. OCTAVE Allegro melibatkan empat fase yang dikelompokkan dalam proses identifikasi risiko, yaitu mendefinisikan pendorong atau pedoman, memprofilkan aset, mengidentifikasi ancaman, serta mengidentifikasi dan mengurangi risiko[7]. Framework ini disusun untuk membantu organisasi, termasuk institusi pendidikan seperti Universitas Islam XYZ, dalam mengidentifikasi aset informasi kritis, menganalisis potensi ancaman, serta merumuskan langkah-langkah

mitigasi yang diperlukan. Penerapan OCTAVE Allegro digunakan untuk penilaian risiko terutama pada sistem informasi kritis kegiatan utama di universitas, seperti Sistem Informasi Akademik[8].

Penelitian ini bertujuan untuk mengevaluasi penerapan OCTAVE Allegro dalam manajemen risiko sistem informasi di Universitas Islam XYZ. Penelitian ini berfokus pada identifikasi risiko, pembagian tanggung jawab, dan evaluasi efektivitas mitigasi risiko. Diharapkan penelitian ini dapat memberikan pengaruh penting dalam peningkatan keamanan informasi di lingkungan akademik khususnya di Universitas Islam. Dengan menerapkan OCTAVE allegro, suatu perguruan tinggi akan mendapatkan pemahaman yang lebih mendalam mengenai risiko yang ada pada sistem informasi akademik [9].

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Manajemen risiko dalam keamanan sistem informasi penting untuk melindungi aset organisasi dari ancaman yang dapat merugikan. Dengan pendekatan sistematis seperti OCTAVE Allegro, organisasi dapat mengidentifikasi dan mengelola risiko secara efektif untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi. Dian Saputro meneliti penerapan OCTAVE Allegro di Puskesmas XYZ untuk mengatasi masalah keamanan informasi yang sering diretas akibat ketiadaan manajemen risiko. Penelitian ini berhasil mengidentifikasi risiko pada data, aplikasi, perangkat keras, perangkat lunak, dan personel, sehingga menghasilkan tata kelola keamanan informasi yang lebih sistematis dan efisien[10].

Khoirun Nadiya dan tim menggunakan OCTAVE Allegro untuk mengidentifikasi risiko pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Ampel. Hasil penelitian menunjukkan bahwa risiko terhadap reputasi, produktivitas, dan keamanan dapat diminimalkan dengan rekomendasi mitigasi berbasis delapan langkah metode Octave Allegro[2]

Kholifah, Reza Ade Putra, Fathiyah Nopriani meneliti pentingnya penilaian risiko terhadap sistem informasi akademik di Universitas Muhammadiyah Palembang untuk meningkatkan keamanan informasi. Penelitian ini menunjukkan bahwa evaluasi risiko yang berkelanjutan sangat penting, terutama dalam konteks institusi pendidikan yang bergantung pada sistem informasi[8].

2.2. Manajemen Risiko

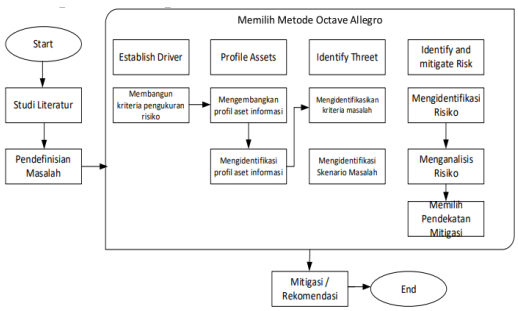
Manajemen risiko adalah proses terstruktur untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang dapat memengaruhi pencapaian tujuan organisasi. Tiga komponen manajemen risiko adalah identifikasi risiko, penilaian risiko, dan pengendalian risiko[11]. Kesuksesan manajemen risiko bergantung pada kemampuan (kapabilitas), cara pandang (persepsi), dan niat (intensi) orang yang terlibat [11].

2.3. OCTAVE ALLEGRO

OCTAVE, juga disebut sebagai Operationally Critical Threat, Asset, and Vulnerability Evaluation adalah serangkaian elemen yang menyeluruh dan terstruktur untuk penilaian risiko keamanan informasi berbasis konteks[10]. Metode Octave Allegro dibuat untuk memberikan penilaian risiko yang komprehensif dengan tujuan mencapai hasil yang tepat tanpa memerlukan pengetahuan rinci tentang penilaian risiko. Kerangka OCTAVE Allegro diterapkan untuk menghimpun data dan informasi terkait manajemen risiko sistem informasi[10].

3. METODE PENELITIAN

Metode dalam penelitian ini dilakukan dengan dua tahap, yaitu tahap penelitian dan tahap pengumpulan data. Tahap penelitian berawal menggunakan kajian pustaka yang kemudian data diperiksa dan diperoleh sebagian dari proses penelitian lapangan staff Universitas Islam XYZ. Tahap pertama adalah penelitian, yang terdiri dari studi literatur, identifikasi masalah, dan penerapan OCTAVE Allegro. Octave Allegro adalah sebuah kerangka kerja yang mengadopsi metode OCTAVE, dirancang untuk menilai risiko terhadap operasi organisasi atau perusahaan terkait aset informasi, hal ini bertujuan untuk memberikan hasil yang lebih cepat tanpa membutuhkan pemahaman yang mendalam tentang penilaian risiko [1]. Tahap ini dilaksanakan melalui studi literatur dengan meninjau literatur yang relevan terkait manajemen risiko sistem informasi dan kerangka kerja OCTAVE Allegro. Selanjutnya, pada Identifikasi Masalah, dilakukan analisis terhadap masalah keamanan yang dihadapi oleh sistem informasi di Universitas Islam XYZ. Selanjutnya, penerapan OCTAVE Allegro, dilakukan analisis risiko secara mendalam dengan menggunakan metode OCTAVE Allegro untuk mengidentifikasi ancaman, risiko, serta mitigasi yang diperlukan guna meminimalkan dampak risiko yang teridentifikasi. Proses ini mencakup identifikasi risiko yang ada dalam operasional sistem informasi universitas. Selanjutnya, solusi untuk permasalahan tersebut akan dirumuskan berdasarkan kerangka kerja OCTAVE Allegro [12].



Gambar 1. Alur Penelitian Octave Allegro

Berdasarkan hasil studi metode Octave Allegro, ditawarkan berbagai solusi dan rekomendasi memperkecil masalah ini[10]. Terdapat beberapa

tahapan penelitian yang dilaksanakan pada Universitas Islam XYZ, tahapan kajian ini dapat dilihat pada Gambar 1.

Tahap kedua adalah pengumpulan data. Langkah ini dilakukan untuk mengumpulkan data dan informasi yang relevan dengan topik pembahasan melalui studi literatur dari berbagai sumber rujukan seperti artikel dan prosiding online serta sumber lainnya. Proses pengumpulan data ini membantu untuk menganalisis masalah, memperoleh informasi terkait landasan teori yang dibutuhkan, menentukan kegunaan dan tujuan masalah, serta mengidentifikasi keterbatasan penelitian. Berdasarkan data yang terkumpul, implementasinya dilakukan dengan menggunakan metode penilaian risiko tahapan spesifik yang termasuk dalam kerangka OCTAVE Allegro [16].

4. HASIL DAN PEMBAHASAN

4.1. Kriteria Pengukuran Resiko

Kriteria pengukuran risiko digunakan untuk menilai seberapa besar dampak dari setiap risiko yang diidentifikasi terhadap berbagai aspek operasional di Universitas Islam XYZ. Hasil analisa yang dilakukan tersaji secara detil pada tabel 1.

Tabel 1. Kriteria Pengukuran Risiko

Lembar Kerja Allegro	**Kriteria Pengukuran Risiko Dan Kepercayaan Stakeholder**
Prioritas	**Area Dampak**
I	Integritas Nilai Islami
II	Keamanan Data Stakeholder
III	Kepercayaan dan Reputasi Stakeholder
IV	Keuangan
V	Produktivitas Akademik

4.2. Sumber Daya Data Profile

Aset informasi yang dipilih adalah yang relevan dalam proses inti Universitas Islam XYZ. Aset informasi kritis akan dicatat pada lembar kerja aset informasi kritis yang telah disediakan oleh OCTAVE Allegromethod. Profil merupakan representasi yang menggambarkan fungsi, karakteristik, kualitas, dan nilai unik dari aset informasi [13]. Hasil analisa yang diperoleh tersaji secara detil pada tabel 2.

Tabel 2. Sumber Daya Data Profile

Allegro Worksheet	**Critical Information Asset Profile**	
Critical asset	Apa saja aset informasi yang penting?	Aset informasi akademik
Rationable for selection	Mengapa informasi tersebut dianggap sebagai aset bagi organisasi?	Karena aset tersebut merupakan pendukung utama dalam kegiatan operasional akademik
Description	Apa deskripsi yang disepakati dari asset informasi ini?	Aset berisi data pribadi mahasiswa dan data perkuliahan mahasiswa (seperti kurikulum, KRS, KHS, transkrip, dan lain-lain)
Owner (s)		Staff Pusat Sistem Teknologi Informasi dan Pangkalan Data
Security recuirements	Apa saja persyaratan keamanan yang diimplementasikan pada aset informasi ini?	
Confidentiality	Hanya pihak berwenang yang dapat mengakses dan memodifikasi data	Mahasiswa dapat mengakses dan memodifikasi data pribadi jika sudah tidak sesuai dengan kenyataan.
Integrity	Data yang dimasukkan harus benar dan sesuai dengan kenyataan.	Mahasiswa dapat mengakses dan memodifikasi data pribadi jika sudah tidak sesuai dengan kenyataan.
Availability	Aset ini harus tersedia setiap hari agar kegiatan operasional akademik tidak terganggu	Sivitas akademika (mahasiswa, dosen dan staff Pusat Sistem Teknologi Informasi dan Pangkalan Data)
Most important security requirement		
Apa persyaratan keamanan terpenting untuk informasi ?		
Kerahasiaan	Integritas	Ketersediaan

4.3. Identifikasi Kontainer dan Aset Informasi

Identifikasi kontainer dan aset informasi merupakan tempat di mana aset informasi disimpan, ditransmisikan atau diproses. Mengamankan aset informasi dari ancaman yang membahayakan dapat meningkatkan keamanan data dalam sistem informasi. Keamanan informasi bertujuan untuk menjaga kerahasiaan, ketersediaan, dan integritas dari sumber daya informasi dalam sebuah perusahaan[15]. Aset informasi dibagi menjadi tiga kategori, yaitu Teknis, Fisik, Orang. Tahap pertama yakni Teknis. Teknis dalam konteks aset informasi mencakup Perangkat keras, perangkat lunak atau sistem yang berada di bawah kendali perusahaan (internal), dan di luar kendali perusahaan (eksternal). Adapun hasil analisa lingkungan risiko aset informasi teknis tersaji dengan detail pada tabel 3.

Tabel 3. Lingkungan Risiko Aset Informasi (Teknis)

Kategori	Deskripsi	Owner
Internal	Web server & Database server	Staff Pusat Sistem Teknologi Informasi dan Pangkalan Data Universitas Islam XYZ
	Komputer & Laptop	Sarpras Universitas Islam XYZ
	Jaringan Internal (LAN)	Staff Pusat Sistem Teknologi Informasi dan Pangkalan Data Universitas Islam XYZ
Eksternal	Internet Service Provider (ISP)	Vendor Pihak Ke-3

Tahap kedua yakni fisik. Fisik dalam konteks aset informasi mencakup lokasi fisik atau dokumen yang berada di bawah kendali perusahaan (internal), dan di luar kendali perusahaan (eksternal). Adapun hasil analisa lingkungan risiko aset informasi fisik tersaji dengan detail pada tabel 4.

Tabel 4. Lingkungan Risiko Aset Informasi (Fisik)

Kategori	Deskripsi	Owner
Internal	Mencetak file kehadiran mahasiswa untuk didistribusikan selama kelas berlangsung	Pihak Akademik

Tahap ketiga yakni orang. Orang dalam konteks aset informasi mencakup Siapapun yang mengetahui informasi yang berada di bawah kendali perusahaan (internal), dan di luar kendali perusahaan (eksternal). Adapun hasil analisa lingkungan risiko aset informasi orang tersaji dengan detail pada tabel 5.

Tabel 5. Lingkungan Risiko Aset Informasi (Orang)

Kategori	Deskripsi	Owner
Internal	Pelaksana Pengelola SI/IT Universitas Islam XYZ	Staff Pusat Sistem Teknologi Informasi dan Pangkalan Data

4.4. Identifikasi Area Masalah

Analisis digunakan untuk mengidentifikasi sejumlah area of concern terkait risiko penggunaan data dalam sistem informasi di Universitas Islam XYZ. Setiap area di dalam tabel merujuk pada potensi masalah yang dapat memengaruhi integritas, keamanan, dan kerahasiaan data pengguna, khususnya data mahasiswa. Hasil analisa yang dilakukan tersaji secara detail pada tabel 6.

Tabel 6. Identifikasi Area Masalah

No	Area of Concern – Pengguna Data
1	Data pengguna yang terdapat pada database Universitas telah rusak.
2	Pelaksanaan hak akses untuk meminta informasi akademik yang sedang dalam proses.
3	Penyalahgunaan hak akses ke data mahasiswa.
4	Pemalsuan data terhadap data mahasiswa.
5	Kebocoran data permintaan user.
6	Pemanfaatan kerentanan dalam akses data eksternal yang tidak terdeteksi dalam sistem keamanan.
7	Kesalahan saat memasukkan data mahasiswa ke dalam sistem akademik Universitas.
8	Kehilangan data pengguna karena kesalahan teknis atau gangguan.

4.5. Identifikasi Skenario Ancaman

Identifikasi skenario ancaman dilakukan untuk mengevaluasi risiko yang dapat memengaruhi manajemen sistem informasi Universitas Islam XYZ, khususnya terkait data mahasiswa. Ancaman ini melibatkan potensi eksploitasi kerentanan oleh pihak internal maupun eksternal yang dapat mengganggu pengelolaan sistem. Evaluasi mencakup aktor, cara, motivasi, serta dampak ancaman, seperti pengungkapan, modifikasi, perusakan, dan gangguan sistem. Hasil analisa identifikasi ancaman tertera dengan detail pada tabel 7.

Tabel 7. Identifikasi Skenario Ancaman

Aset Informasi	Data Mahasiswa
Area perhatian	Pemanfaatan kerentanan dalam akses pihak eksternal dan internal yang tidak diketahui identitasnya terhadap manajemen sistem informasi.
1. Actor	Mahasiswa
2. Means	Eksploitasi kerentanan di server, database, atau modul manajemen sistem oleh pihak eksternal dan internal.
3. Motives	Sengaja dan tidak sengaja.
4. Outcome	[✓] Disclosure [✓] Modification [✓] Destruction [✓] Interruption
5. Security Requirement	Meningkatkan pengelolaan sistem informasi melalui peningkatan keamanan perangkat lunak, perangkat keras, dan jaringan. Pemeriksaan secara berkala terhadap sistem manajemen Universitas Islam XYZ diperlukan.
6. Probability	[✓] High [✓] Medium [✓] Low

4.6. Identifikasi Risiko

Identifikasi risiko dilakukan untuk mengevaluasi berbagai area of concern yang dapat memengaruhi pengelolaan sistem informasi Universitas Islam XYZ. Risiko-risiko ini berkaitan dengan potensi masalah dalam manajemen data mahasiswa, seperti pemanfaatan celah sistem, kerusakan data, serta kesalahan dalam proses input data. Hasil analisa identifikasi risiko tertera dengan detail pada tabel 8.

Tabel 8. Identifikasi Risiko

No	*Area of Concern*	*Consequences*
1	Pemanfaatan celah keamanan dalam manajemen SI oleh pihak luar maupun internal.	Informasi dapat dimodifikasi secara tidak sah, mengganggu proses pengelolaan data dan operasi sistem informasi Universitas.
2	Penggunaan hak akses secara tidak sah terhadap data mahasiswa.	Ancaman terhadap keamanan data mahasiswa, berisiko memengaruhi kepercayaan dan menyebabkan korupsi data penting.
3	Data mahasiswa di database Universitas Islam telah rusak.	Rusaknya data mahasiswa menyebabkan gangguan terhadap keutuhan informasi dan kelancaran proses akademik.
4	Kehilangan data mahasiswa akibat tidak melakukan backup (pencadangan).	Gangguan pada proses akademik dan kerugian signifikan akibat hilangnya data penting mahasiswa.
5	Pemalsuan informasi data mahasiswa.	Kesalahan informasi dapat menurunkan kepercayaan pada sistem informasi Universitas dan mempengaruhi proses administrasi.
6	Kesalahan dalam input data mahasiswa ke dalam sistem Universitas Islam.	Kesalahan input data dapat merugikan mahasiswa dan mengganggu proses operasional administrasi akademik.
7	Kebocoran data permintaan pengguna.	Informasi sensitif yang bocor dapat dimanfaatkan oleh pihak yang tidak berwenang, merugikan pihak Universitas dan mahasiswa.

4.7. Analisis Risiko

Pada tahap analisis risiko, area dampak yang relevan dengan manajemen sistem informasi Universitas Islam XYZ ditentukan berdasarkan prioritas yang telah diidentifikasi. Tabel analisis risiko Universitas Islam XYZ digunakan untuk mengukur skor risiko berdasarkan dampak pada Integritas Nilai Islami, Keamanan Data Stakeholder, Kepercayaan dan Reputasi Stakeholder, Keuangan, dan Produktivitas Akademik. Setiap area dampak memiliki prioritas yang berbeda dan dikategorikan dalam tiga tingkat pengaruh: rendah, sedang, dan tinggi. Hasil analisa risiko tertera dengan detail pada tabel 9.

Tabel 9. Score Analisis Risiko

Area Dampak	Prioritas	Skor Area Dampak		
		Rendah (n=(1))	Sedang (n=(2))	Tinggi (n=(3))
Integritas Nilai Islami	I	1	3	5
Manajemen Data Stakeholder	II	2	4	7
Kepercayaan dan Reputasi Stakeholder	III	3	6	9
Keuangan	IV	4	7	10
Produktivitas Akademik	V	5	8	12

4.8. Pendekatan Mitigasi

Berdasarkan analisis faktor pada langkah akhir ini dengan menggunakan pendekatan mitigasi, semua risiko yang teridentifikasi ditetapkan berdasarkan skor risiko relatif[10]. Matriks relatif risiko digunakan untuk mengklasifikasikan tingkat risiko yang telah diidentifikasi. Pendekatan mitigasi disesuaikan dengan skor risiko, dibagi menjadi tiga kategori: mengurangi, menunda, dan menerima. Risiko diterima jika diperkirakan memiliki dampak yang minimal terhadap bisnis. Risiko dimitigasi dengan mengambil tindakan pencegahan untuk mengurangi tingkat risiko hingga mencapai level yang dapat diterima, sementara risiko dapat ditangguhkan dengan mengumpulkan lebih banyak data tentang sistem untuk analisis lebih lanjut[14]. Klasifikasi ini memberikan panduan untuk menentukan tindakan mitigasi yang tepat berdasarkan tingkat urgensi risiko. Hasil analisa matriks relatif risiko tertera dengan detail pada tabel 10.

Tabel 10. Matriks Relatif Risiko

Matriks Relatif Risiko		
Skor Risiko	**POOL**	**Pendekatan Mitigasi**
30 – 45	1	Mengurangi
16 – 29	2	Menunda
0 – 15	3	Menerima

Tabel 11 menunjukkan hasil identifikasi dan analisis risiko yang telah dipetakan ke dalam matriks relatif risiko. Setiap area perhatian dianalisis untuk menentukan pendekatan mitigasi yang paling sesuai, baik itu mengurangi, menunda, atau menerima risiko. Hasil ini membantu menentukan prioritas tindakan mitigasi yang perlu diambil.

Tabel 11. Mitigasi

No	Area yang Menjadi Perhatian	Matriks Relatif Risiko	POOL	Pendekatan Mitigasi
1	Pemanfaatan celah keamanan dalam manajemen SI oleh pihak luar maupun internal.	37	1	Mengurangi
2	Penggunaan hak akses secara tidak sah terhadap data mahasiswa.	29	2	Menunda
3	Data mahasiswa di database Universitas Islam telah rusak.	40	1	Mengurangi
4	Kehilangan data mahasiswa akibat tidak melakukan backup (pencadangan)	44	1	Mengurangi

No	Area yang Menjadi Perhatian	Matriks Relatif Risiko	POOL	Pendekatan Mitigasi
5	Pemalsuan informasi data mahasiswa.	43	1	Mengurangi
6	Kesalahan dalam input data mahasiswa ke dalam sistem Universitas Islam.	15	3	Menerima
7	Kebocoran data permintaan pengguna.	36	1	Mengurangi

Berdasarkan hasil analisis risiko, rekomendasi kontrol disarankan untuk mengatasi risiko dengan cara mengurangi atau menghilangkan risiko yang telah teridentifikasi pada langkah sebelumnya[7]. Tabel 12 memberikan rincian kontrol yang diambil untuk masing-masing area perhatian, beserta deskripsinya, guna meningkatkan keamanan dan efektivitas manajemen sistem informasi Universitas Islam XYZ.

Tabel 12. Kontrol dan Rekomendasi

No	Wilayah Perhatian	Rekomendasi	Deskripsi
1	Pemanfaatan celah keamanan dalam manajemen SI oleh pihak luar maupun internal.	RA-3 Risk Assessment	Menganalisis dan mendokumentasikan ancaman pada kerentanan manajemen data baik internal maupun eksternal.
2	Penggunaan hak akses secara tidak sah terhadap data mahasiswa.	PE-2 Physical Access Control	Melakukan pemeriksaan dan pemantauan akses terhadap data mahasiswa.
3	Data mahasiswa di database Universitas Islam telah rusak.	CP-2 Contingency Plan	Mempunyai rencana cadangan sebagai solusi dari kehilangan data, termasuk penyiapan backup data.
4	Kehilangan data mahasiswa akibat tidak melakukan backup (pencadangan).	Information System Backup	Melakukan backup secara berkala untuk menjaga kerahasiaan, integritas, dan ketersediaan cadangan.
5	Pemalsuan informasi data mahasiswa.	AC-4 Information Flow Enforcement	Melakukan pemantauan aliran informasi dan peninjauan terkait modifikasi pada data mahasiswa.
6	Kesalahan dalam input data mahasiswa ke dalam sistem Universitas Islam.	IR-4 Incident Handling	Melakukan validasi dan pemeriksaan input data mahasiswa secara menyeluruh.
7	Kebocoran data permintaan pengguna	IA-2 Identification Authentication	Melakukan verifikasi ulang terhadap pengguna yang meminta akses data mahasiswa.

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil menunjukkan bahwa penerapan OCTAVE Allegro dalam manajemen risiko sistem informasi di Universitas Islam XYZ efektif dalam mengidentifikasi, menilai, dan mengurangi risiko yang terkait dengan data akademik dan manajemen sistem informasi. Dari hasil analisis, ditemukan beberapa risiko utama seperti kerentanan dalam akses data, kesalahan input, dan potensi kebocoran data. Dengan menggunakan OCTAVE Allegro, risiko-risiko tersebut dapat dimitigasi dengan baik, terutama melalui pendekatan mitigasi seperti mengurangi, menunda, dan menerima. Hasil penelitian ini menunjukkan bahwa metode OCTAVE Allegro mampu meningkatkan keamanan dan manajemen sistem informasi Universitas Islam XYZ, yang pada akhirnya berdampak positif pada operasional dan reputasi universitas.

DAFTAR PUSTAKA

[1] 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," *J. Comput. Inf. Syst. Ampera*, vol. 4, no. 1, pp. 44–54, 2023, doi: 10.51519/journalcisa.v4i1.337.

[2] K. Nadiya, N. C. Nisa, S. A. N. Aini, and A. U. P. S. Jandi, "Analisis Manajemen Risiko Pada Sistem Informasi Akademik Menggunakan Framework OCTAVE ALLEGRO," *JORAPI J. Res. Publ. Innov.*, vol. 2, no. 2, pp. 1479–1491, 2024, [Online]. Available: https://jurnal.portalpublikasi.id/index.php/JORAPI/index

[3] J. Simangunsong, N. Hutagaol, and F. A. Pasaribu, "Implementasi Aplikasi Internal Service Order (ISO) Berbasis Web pada Perusahaan Manufaktur Furniture," *J. Inform. J. Pengemb. IT*, vol. 9, no. 2, pp. 151–163, 2024, doi: 10.30591/jpit.v9i2.6813.

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

[5] F. Mahardika, A. Guntara, A. Saeppani, D. Indra, and M. Suryadi, "Evaluation, Dapodik Systems, OCTAVE-S, Risk Management.," 2020, doi: 10.4108/eai.11-7-2019.2297555.

[6] 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.

[7] H. Sulaeman, H. P. Utomo, and A. I. Suryana, "Penilaian Risiko Keamanan Informasi Pada

Sistem Informasi Akademik (Siakad) Dengan Menggunakan Framework Nist-Sp 800 30," *Naratif J. Nas. Riset, Apl. dan Tek. Inform.*, vol. 5, no. 2, pp. 171–185, 2023, doi: 10.53580/naratif.v5i2.254.

[8] K. Kholifah, R. A. Putra, and F. Nopriani, "Analisis Penilaian Risiko Terhadap Penggunaan Sistem Informasi Akademik Pada Universitas Muhammadiyah Palembang Menggunakan Metode Octave Allegro," *J. Comput. Inf. Syst. Ampera*, vol. 2, no. 1, pp. 28–42, 2021, doi: 10.51519/journalcisa.v2i1.58.

[9] 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.

[10] D. Saputra, "ANALISIS DAN PENGELOLAAN RISIKO KEAMANAN INFORMASI PUSKESMAS MENGGUNAKAN METODE OCTAVE ALLEGRO (STUDI KASUS : PUSKESMAS XYZ)," vol. 2, no. 1, pp. 12–18, 2024.

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

[12] 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.

[13] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," May 2007. Accessed: Oct. 04, 2022. [Online]. Available: http://www.sei.cmu.edu/publications/pubweb.html

[14] A. I. Awad, M. Shokry, A. A. M. Khalaf, and M. K. Abd-Ellah, "Assessment of potential security risks in advanced metering infrastructure using the OCTAVE Allegro approach," *Comput. Electr. Eng.*, vol. 108, no. December 2022, p. 108667, 2023, doi: 10.1016/j.compeleceng.2023.108667.

[15] A. Wijoyo, S. Fatimah, and Y. Widianti, "Keamanan Data dalam Sistem Informasi Manajemen: Risiko dan Strategi Perlindungan," *... J. Teknol. Bisnis ...*, vol. 1, no. 2, pp. 1–7, 2023, [Online]. Available: http://jurnalmahasiswa.com/index.php/teknobis/article/view/441

[16] 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.