DOI: https://doi.org/10.62017/tektonik

Analisis Risiko Keamanan Aset Informasi pada Sistem Informasi Akademik menggunakan Metode Octave Allergro

Shaubil haq *[1]
Kasmawi [2]

[1,2] Politeknik Negeri Bengkalis
*e-mail: shaubilhaq4@gmail.com[1] mawipb@gmail.com

Abstrak

Penelitian ini dilakukan untuk mengevaluasi risiko yang dihadapi oleh sistem informasi akademik (SIAKAD) Politeknik Negeri Bengkalis. SIAKAD digunakan untuk mendukung kegiatan layanan akademik dengan teknologi informasi yang baik. Namun, dalam aplikasinya, SIAKAD mengalami beberapa kendala, terutama terkait dengan kerusakan perangkat keras atau server yang dapat mempengaruhi aktivitas SIAKAD. Penelitian ini menggunakan metode Octave Allegro dan dilakukan dalam 8 langkah yang meliputi menetapkan kriteria penilaian risiko, mengembangkan profil aset informasi, memanggil kontainer informasi aset, mengidentifikasi area kekhawatiran, membantu skenario bantuan, analisis risiko, dan pendekatan penanganan. Data diperoleh dari 2 responden melalui observasi dan wawancara,. Hasil penelitian menunjukkan bahwa terdapat 4 ancaman risiko yang dihadapi oleh SIAKAD Politeknik Negeri Bengkalis, dengan 4 risiko yang memerlukan tindakan pengurangan risiko (mitigasi) Penelitian ini diharapkan dapat memberikan informasi yang berguna bagi pengembangan SIAKAD dan pengelolaan risiko yang lebih efektif di Politeknik Negeri Bengkalis dan institusi serupa lainnya.

Kata Kunci: *Aset Infomasi , Keamanan, Octave Allergro, Sistem Informasi*

Abstract

This research was conducted to evaluate the risks faced by the Bengkalis State Polytechnic academic information system (SIAKAD). SIAKAD is used to support academic service activities with good information technology. However, in its application, SIAKAD experienced several problems, especially related to hardware or server damage which could affect SIAKAD's activities. This research uses the Octave Allegro method and is carried out in 8 steps which include establishing risk assessment criteria, developing information asset profiles, calling asset information containers, identifying areas of concern, assisting assistance scenarios, risk analysis, and handling approaches. Data was obtained from 2 respondents through observation and interviews. The results of the research show that there are 4 risk threats faced by SIAKAD Bengkalis State Polytechnic, with 4 risks requiring risk reduction (mitigation) action. This research is expected to provide useful information for the development of SIAKAD and more effective risk management at Bengkalis State Polytechnic and institutions other similar.

Keywords*:* Information Assets, Information Systems, Octave Allegro, Security

PENDAHULUAN

Sistem Informasi Akademik banyak digunakan oleh hampir semua Kampus khususnya di Indonesia, ini bertujuan untuk mempermudah pengiriman Informasi untuk mahasiswa, staf pengajar dan staf administrasi manajemennya. Semakin banyak sistem berinteraksi dengan pengguna, semakin banyak sistem akan mudah diretas atau dirusak oleh pihak-pihak yang tidak bertanggung jawab. Hal ini akan menjadi masalah baru dalam hal keamanan. Sistem informasi salah satu bagian penting dalam suatu proses bisnis di lembaga pendidikan. Apabila suatu permasalahan muncul pada suatu sistem informasi maka akan menghambat proses bisnis yang berjalan di dalam Kampus. Tujuan utama dari proses analisis resiko keamanan adalah untuk melindungi organisasi sehingga dapat dengan maksimal dalam menjalankan visi dan misi organisasi, bukan hanya sekedar aset teknologi informasi saja [1].

Octave Allegro merupakan salah satu metode manajemen resiko sistem informasi yang dapat diterapkan pada perguruan tinggi tanpa memerlukan keterlibatan yang ekstensif di dalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam

DOI: https://doi.org/10.62017/tektonik

mencapai misi dan tujuannya. Metode octave allegro adalah penilaian yang luas terhadap lingkungan risiko operasional suatu organisasi dengan tujuan menghasilkan yang lebih baik tanpa perlu pengetahuan yang luas dalam hal penilaian risiko. Oleh karena itu kerangka kerja manajemen risiko yaitu octave allegro, salah satu kerangka kerja yang dibutuhkan dalam analisis risiko yang baik [2].

Politeknik Negeri Bengkalis merupakan perguruan tinggi vokasi yang bergerak pada bidang pendidikan. Politeknik Negeri Bengkalis merupakan salah satu perguruan tinggi vokasi yang ada di Riau yang beralamatkan di jalan Bathin Alam, Sungai Alam Kabupaten Bengkalis. Dalam proses bisninya yang mana telah memanfaatkan Sistem untuk mengelola data akademik yang sering dikenal dengan SIAKAD (Sistem Informasi Akademik) berbasis web. SIAKAD merupakan sistem informasi akademik pada perguruan tinggi di Politeknik Negeri Bengkalis, SIAKAD ini digunakan pertama kali pada tahun 2022 dan memiliki beberapa fitur antara lain mulai dari pengambilan mata kuliah dan mencetaknya, melihat kartu hasil study (KHS), serta melihat informasi tentang pengumuman terkait kemahasiswaan dan perkuliahan. Tujuan dari penerapan SIAKAD antara lain yaitu untuk memudahkan proses akademik baik untuk dosen maupun mahasiswa, serta memudahkan staf dalam mengelola KRS, KHS dan lainnya kepada mahasiswa [1].

Dalam menunjang pelayanan pendidikan, khususnya pada pelayanan akademik yang merupakan salah satu sektor inti pada perguruan tinggi karena merupakan proses bisnis utama. Pelayanan akademik yang cepat dan tepat tidak lepas dari teknologi informasi yang baik dan benar. Demi mewujudkan sistem informasi akademik dengan pelayanan yang maksimal tentunya harus diimbangi dengan teknologi yang baik pula. Risiko merupakan potensial peristiwa yang berpotensi berbahaya karena ketidakpastian terjadinya suatu peristiwa. Politeknik Negeri Bengkalis sebelumnya belum ada penelitian yang meneliti mengenai risiko khususnya penilaian resiko keamanan sistem informasi pada sistem informasi akademik Politeknik Negeri bengkalis. Sehinga Politeknik Negeri Bengkalis belum mengetahui kemungkinan risiko dan tingkat keamanan pada SIAKAD dan belum maksimal dalam persiapan untuk menanggulangi dampak risiko yang akan terjadi [3].

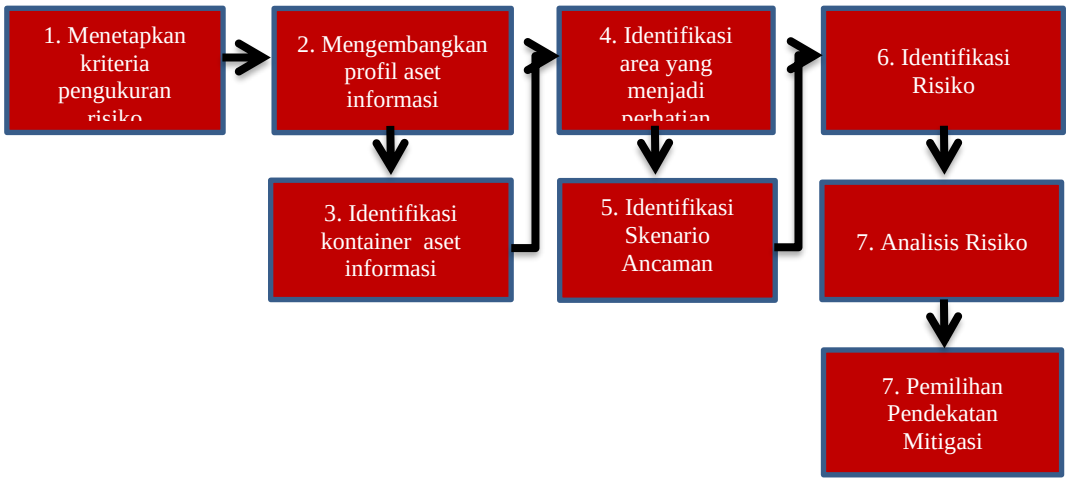
Metode ini berfokus pada aset informasi organisasi. OCTAVE Allegro telah dilengkapi dengan guidance, lembar kerja hingga kuesioner. OCTAVE Allegro adalah proses yang disederhanakan dengan memberikan hasil penilaian risiko yang kuat dengan investasi waktu dan sumber daya yang lebih kecil dan tidak memerlukan keamanan sistem informasi yang luas atau pengalaman manajemen risiko[4].

OCTAVE Allegro dikembangkan bertujuan untuk membantu organisasi memastikan bahwa kegiatan keamanan informasi mereka selaras dengan tujuan organisasi. Dengan menerapkan analisis risiko atau penilaian risiko pada keamanan sistem informasi diharapkan dapat mengurangi dampak risiko yang akan terjadi, sehingga analisis risiko sistem informasi sangat penting untuk di implementasikan pada Politeknik Negeri Bengkalis. Berdasarkan uraian permasalahan diatas maka penelitian ini menghasilkan sebuah rekomendasi Penilaian Risiko yang telah di identifikasi pada Sistem Informasi Akademik Politeknik Negeri Bengkalis menggunakan Metode Octave Allegro[4].

METODE

Menetapkan Driver	Profil Aset	Mengidentifikasi ancaman	Mengidentifikasi dan melakukan mitigasi

Vol. 2, No. 1 Oktober 2024, Hal. 192-202
DOI: https://doi.org/10.62017/tektonik



Gambar 3.1 Prosesur penelitian [11].

Keterangan gambar OCTAVE Allegro terdiri dari delapan langkah :

1. Langkah 1 – Membangun Kriteria Pengukuran Risiko, Di dalam langkah ini terdapat dua aktivitas, diawali identifikasi kriteria pengukuran risiko dan memberikan prioritas sesuai tingkat kepentingan menggunakan *impact area ranking worksheet*
2. Langkah 2 – Mengembangkan Profil Aset Informasi, Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai information aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi aset informasi kritis kemudian mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk *confidentiality, integrity dan availaibility*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.
3. Langkah 3 – Mengidentifikasi Kontainer dari Aset Informasi, Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi dilindung, tingkat perlindungan atau pengaman aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.
4. Langkah 4 – Mengidentifikasi Area Masalah, Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi.
5. Langkah 5 – Mengidentifikasi Skenario Ancaman, Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan *Appendix C – Threat Scenarios Questionnaries.*
6. Langkah 6 – Mengidentifikasi Risiko, Aktivitas satu pada langkah 6 menentukan threat scenario yang telah didokumentasikan.
7. Langkah 7 – Menganalisis Risiko, Aktivitas satu dimulai dengan melakukan review risk measurement criteria dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

DOI: https://doi.org/10.62017/tektonik

8. Langkah 8 – Memilih Pendekatan Pengurangan, Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasaarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

HASIL DAN PEMBAHASAN

Hasil Pembahasan

Dari hasil identifikasi dan penilaian risiko maka berikut beberapa kontrol objektif dari standar ISO 27001 yang direkomendasikan untuk penanganan potensi risiko-risiko yang telah diidentifikasi.

Tabel 4. 1 Rekomendasi kontrol Risiko

No	Information Asset	Threat Scenarios	Risk Handling	Control Recommendation
1	Aset Jaringan	Terjadinya kendala listrik mati	Diperlukan penanganan segera.	Lakukan pencadangan arus listrik sementara untuk mengatasi terjadinya gangguan kendala pada sistem siakad, contohnya menerapkan UPS.
2	Aset Staf Admin	Terjadinya kesalahan input data oleh staff admin	Aktivitas dapat dijalankan dengan penambahan kontrol.	Pastikan staf admin telah menerima pelatihan yang memadai dan memiliki sistem validasi data yang kuat untuk mengurangi kesalahan input data.
3.	Data Mahasiswa	Penyalahgunaan back-up data oleh mahasiswa	Aktivitas dapat diterima/belum pernah terjadi	Pastikan untuk memberikan akses hanya kepada personel yang berwenang dan relevan, serta tetap memantau aktivitas akses dan penggunaan data secara teratur untuk mendeteksi potensi penyalahgunaan.
4.	Staf Admin	Penyalahgunaan user akses oleh pihak lain yang tidak bertanggung jawab	Diperlukan penanganan segera.	Pastikan untuk menerapkan otentikasi dua faktor dan membatasi akses hanya kepada pengguna yang membutuhkannya untuk mengurangi risiko penyalahgunaan akses pengguna oleh pihak yang tidak bertanggung jawab.

Vol. 2, No. 1 Oktober 2024, Hal. 192-202
DOI: https://doi.org/10.62017/tektonik

Pembahasan

3.1 Membangun Kriteria Pengukuran Risiko

Pada langkah 1, menentukan area dampak dan menentukan prioritaskannya. Prioritas yang paling penting diberi nilai 5 dan seterusnya dengan urutan terendah.

Tabel 4. 2 Skala prioritas area dampak

Impact Area	Priority	Nilai Dampak		
		Rendah (1)	Sedang (2)	Tinggi (3)
Produktivitas	1	5	10	15
Reputasi dan kepercayaan	2	4	8	12
Financial	3	3	6	9
Akurasi Data	4	2	4	8
Keamanan	5	1	2	3

Tabel 4. 3 Skala perhitungan

		rendah	sedang	tinggi
Keamanan	5	5	10	15
Akurasi Data	4	4	8	12
Financial	3	3	6	9
Reputasi dan kepercayaan	2	2	4	6
Produktivitas	1	1	2	3
		1	2	3

3.2 Mengembangkan Profil Aset Informasi

Pada langkah 2, dilakukan dengan menggunakan panduan lembar kerja 8. Menentukan dan mengumpulkan informasi mengenai aset informasi yang terdapat pada sistem informasi akademik.

Tabel 4. 4 Profil Aset Informasi Kritis

Allegro Worksheet 2	**PROFIL ASET KRITIS**	
(1) Aset Kritikal Nama asset informasi kritis?	**(2) Rasional Seleksi** Kenapa asset informasi ini penting bagi instansi?	**(3) Deskripsi** Descripsi asset informasi ini?
Aset sistem Akademik	Karena apabila aset data informasi ini hilang dapat di salahgunakan, serta aset sistem informasi akademik berisikan data yang mendukung proses utama dalam kegiatan operasional akademik politeknik negeri bengkalis.	Aset informasi ini terdapat data mahasiswa(biodata, KRS, KHS, Transkip Nilai), tugas, referensi, absensi, data dosen dan karyawan
(4) Pemilik(s) Siapa pemilik asset informasi ini ?		
Mahasiswa, Dosen, Admin siakad, UPT.KJSI		
(5) Persyaratan Keamanan		

DOI: https://doi.org/10.62017/tektonik

Apasaja aspek keamanan informasi yang dibutuhkan oleh asset ini?		
▪ Kerahasiaan	Hanya yang berhak boleh melihat informasi ini	
▪ Integritas	Hanya pegawai tertentu yang boleh mengubah informasi ini	
▪ Ketersediaan	Asset ini harus tersedia 24 jam. 7 hari/minggu	
▪ Other		
(6) Persyaratan Keamanan Paling Penting keamanan apa yang paling penting untuk aset informasi ini?		
4. Confidentiality 5. Integrity 6. Availability		

3.3 Identifikasi Wadah Aset Informasi

Pada langkah ini berfokus pada tempat aset informasi disimpan, dipindahkan, dan diproses. Kontainer aset informasi meliputi aspek fisik, aspek teknik dan aspek pengguna

Tabel 4. 5 Peta Lingkungan Risiko Aset Informasi (Teknik)

Allegro Worksheet 3	IDENTIFIKASI (PEMETAAN) INFORMASI RISIKO LINGKUNGAN ASET KRITIS (PENGGUNA)
Internal	
Deskripsi Wadah	Pemilik
1. Module : Database layanan sistem informasi akademik didalam server yang terdiri dari aset informasi akademik yang digunakan di Divisi IT, admin, dosen dan mahasiswa dalam menggunakan layanan	UPT.KJSI
2. Server : digunakan sebagai media penyimpanan aplikasi dan database dengan menggunakan jaringan internet	
3. Perangkat jaringan : kabel fiber *Optic, Terminal, Router, Switch/hub,* dan *acces point*	
4. Jaringan internet internal : LAN	
5. Komputer : Perangkat komputer server	
6. Sistem Operasi Server : Windows Server	
7. Aplikasi : Sistem Informasi Akademik	
External	
Deskripsi Wadah	Pemilik
Jaringan Internet : Menggunakan Vendor pihak ketiga	Indihome
	My Republik

3.4 Mengidentifikasi Area Perhatian

Pada langkah ini akan disajikan dengan pernyataan deskriptif yang menjelaskan kondisi dan situasi yang dapat mempengaruhi aset informasi.

Vol. 2, No. 1 Oktober 2024, Hal. 192-202
DOI: https://doi.org/10.62017/tektonik

Tabel 4. 6 Area Perhatian

No	**Area Perhatian**	**Aset Terkait**
1	Listrik mati	Jaringan
2	Kesalahan input data	Staf admin
3	Penyalahgunaan back up data mahasiswa	Data mahasiswa
4	Penyalahgunaan user akses oleh pihak lain yang tidak bertanggung jawab	Staf admin

3.5 Mengidentifikasi Skenario Ancaman

Pada tahap ini, dilakukan identifikasi skenario ancaman dengan memberikan gambaran secara detail mengenai properti dari ancaman (actor, means, motivies, outcome, dan security) untuk setiap area of concern.

Tabel 4. 7 Skenario Ancaman

Allegro Worksheet		INFORMASI LEMBAR KERJA RISIKO ASET	
Risiko Aset Informasi	Ancaman	Informasi Aset	Aset sistem informasi akademik
		Area Perhatian	Listrik mati yang menghambat jalannya siakad
		(1) Aktor Siapa yang akan mengeksploitasi wilayah yang menjadi perhatian atau ancaman?	Pihak luar
		(2) cara Bagaimana aktor tersebut melakukannya? Apa yang akan mereka lakukan?	Tidak adanya pasokan listrik sehingga menghambat jalanya siakad
		(3) Motif Apa alasan aktor melakukan hal tersebut?	sengaja
		(4) Hasil Apa dampak yang dihasilkan terhadap aset informasi?	✓ *Interruption loss*
		(5) Persyaratan Keamanan Bagaimana persyaratan keamanan aset informasi dapat dilanggar?	Aset ini harus tersedia
		(6) Probabilitas Seberapa besar kemungkinan skenario ancaman ini bisa terjadi?	Rendah - kemungkinan terjadi listrik mati jarang terjadi
	(7) Konsekuensi		(8) Tingkat Keparahan

DOI: https://doi.org/10.62017/tektonik

	Apa konsekuensi terhadap organisasi atau pemilik aset informasi sebagai akibat dari hasil dan pelanggaran persyaratan keamanan?	Seberapa parah dampaknya terhadap organisasi atau pemilik aset berdasarkan area dampaknya?		
		Area Terdampak	**Nilai**	**Skor**
		Reputasi dan Kepercayaan	sedang	6
		Produktivitas	sedang	3
		Keuangan	Sedang	5
		Keamanan	Rendah	2
		Akurasi Data		9
			Relatif Skor Risiko	25

3.6 Mengidentifikasi Risiko

Pada tahap ini, menentukan dampak dari skenario ancaman. Setiap skenario yang telah dibuat ditentukan juga konsekuensi atau dampak yang mungkin akan ditimbulkan ketika ancaman terjadi.

Tabel 4. 8 skenario ancaman

Allegro Worksheet		INFORMASI LEMBAR KERJA RISIKO ASET		
Risiko Aset Informasi	Ancaman	Informasi Aset	Aset sistem informasi akademik	
		Area Perhatian	Kesalahan input data	
		(1) Aktor Siapa yang akan mengeksploitasi wilayah yang menjadi perhatian atau ancaman?	Staf Admin	
		(2) cara Bagaimana aktor tersebut melakukannya? Apa yang akan mereka lakukan?	Kurang teliti	
		(3) Motif Apa alasan aktor melakukan hal tersebut?	Tidak ssengaja	
		(4) Hasil Apa dampak yang dihasilkan terhadap aset informasi?	✓ *Interruption loss*	
		(5) Persyaratan Keamanan Bagaimana persyaratan keamanan aset informasi dapat dilanggar?	Aset ini harus tersedia	
		(6) Probabilitas Seberapa besar kemungkinan skenario ancaman ini bisa terjadi?	Rendah - kemungkinan terjadi jarang terjadi	
		(7) Konsekuensi Apa konsekuensi terhadap organisasi atau pemilik aset informasi sebagai akibat dari hasil	(8) Tingkat Keparahan Seberapa parah dampaknya terhadap organisasi atau pemilik aset berdasarkan area dampaknya?	
			Area Terdampak	**Nilai**	**Skor**

	dan pelanggaran persyaratan keamanan?			
		Reputasi dan Kepercayaan		6
		Produktivitas		2
		Keuangan		6
		Keamanan		4
		Akurasi Data		8
			Relatif Skor Risiko	26

Allegro Worksheet	INFORMASI LEMBAR KERJA RISIKO ASET			
Risiko Aset Informasi	Ancaman	Informasi Aset	Aset sistem informasi akademik	
		Area Perhatian	Penyalahgunaan user akses oleh pihak lain yang	
		(1) Aktor Siapa yang akan mengeksploitasi wilayah yang menjadi perhatian atau ancaman?	Staf Admin	
		(2) cara Bagaimana aktor tersebut melakukannya? Apa yang akan mereka lakukan?	Kurang teliti	
		(3) Motif Apa alasan aktor melakukan hal tersebut?	Dengan sengaja untuk mengambil data	
		(4) Hasil Apa dampak yang dihasilkan terhadap aset informasi?	✓ *Interruption loss* ✓ *modification*	
		(5) Persyaratan Keamanan Bagaimana persyaratan keamanan aset informasi dapat dilanggar?	User wajib melakukan penggantian password akses secara berkala dan tidak boleh memberitahukan password kepada orang lain.	
		(6) Probabilitas Seberapa besar kemungkinan skenario ancaman ini bisa terjadi?	Rendah - kemungkinan terjadi jarang terjadi	
	(7) Konsekuensi Apa konsekuensi terhadap organisasi atau pemilik aset informasi sebagai akibat dari hasil dan pelanggaran persyaratan keamanan?		(8) Tingkat Keparahan Seberapa parah dampaknya terhadap organisasi atau pemilik aset berdasarkan area dampaknya?	
			Area Terdampak	**Nilai**	**Skor**
	Perusahaan mengalami kerugian apabila pelaku penyalahgunaan membuat kerusakan data karena data menjadi tidak akurat dan		**Reputasi dan Kepercayaan**	medium	6
			Produktivitas	medium	4
			Keuangan	medium	6

DOI: https://doi.org/10.62017/tektonik

	menyebabkan selisih penjualan	**Keamanan**	low	5
		Akurasi Data	low	4
			Relatif Skor Risiko	25

Tabel 4. 9 Relative Risk Matrix

Matriks Skor Risiko Relatif			
Kemungkinan	**Skor Risiko**		
	30 to 45	**16 to 29**	**0 to 15**
Tinggi	Pool1	Pool2	Pool3
Sedang	Pool 2	Pool 2	Pool 3
Rendah	Pool 3	Pool 3	Pool 4

Tabel 4. 10 Pendekatan Mitigasi

POOL	**Pendekatan Mitigasi**
(30 to 45)	Mitigate atau Ditangguhkan
(16 to 30)	Mitigasi
(0 to 15)	Diterima

Tabel 4. 11 Hasil Mitigasi Risiko

Mitigasi risiko	
Area Perhatian	**Pendekatan Mitigasi**
Listrik Mati	Mitigasi
Kesalahan Input data	Mitigasi
Penyalahgunaan back-up data mahasiswa	Mitigasi
Penyalahgunaan user akses oleh pihak yang tidak bertanggung jawab	Mitigasi

KESIMPULAN

1. Untuk melakukan penilaian dan pemberian rekomendasi kontrol keamanan informasi pada siakad dapat digunakan metode OCTAVE allegro.
2. Urutan prioritas area dampak pada siakad secara berturut-turut adalah reputasi dan kepercayaan, produktivitas dan keamanan data.
3. Dari analisis profil aset, aset informasi yang paling critical pada siakad adalah aplikasi mobile siakad dan sistem management siakad, dengan persyaratan keamanan yang paling penting adalah integrity dan availability.
4. Untuk asset informasi aplikasi siakad diketahui bahwa risiko yang dapat terjadi diantaranya adalah Untuk asset informasi aplikasi siakad diketahui bahwa risiko yang dapat terjadi diantaranya adalah Terjadinya kendala listrik mati), Terjadinya kesalahan input data oleh staff admin, Penyalahgunaan back-up data oleh mahasiswa dan Penyalahgunaan user akses oleh pihak lain yang tidak bertanggung jawab.

DOI: https://doi.org/10.62017/tektonik

DAFTAR PUSTAKA

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," vol. 10, no. 2, pp. 488–496, 2023, doi: 10.30865/jurikom.v10i2.5950.

A. Zulfia, E. L. Ruskan, and P. Putra, "Penilaian Risiko Aset Informasi dengan Metode OCTAVE Allegro: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya," JOINS (Journal Inf. Syst., vol. 6, no. 1, pp. 40–47, 2021, doi: 10.33633/joins.v6i1.4088.

a. ไทรทับทิม et al., "Menggunakan Metode Octave Dan Kontrol Iso 27001 Pada Dinas Perhubungan Risk Analysis Using Octave Method and Control Iso 27001 in the Departement of Transportation Communication and Information," J@Ti Undip J. Tek. Ind., vol. 9, no. 2, pp. 3345–3356, 2016, [Online]. Available: http://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf

B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," J. Teknol. dan Inf., vol. 12, no. 2, pp. 106–117, 2022, doi: 10.34010/jati.v12i2.6829.

B. L. Mahersmi, M. F. Artowini, and B. C. Hidayanto, "Analisis Risiko Keamanan Informasi dengan Menggunakan Metode OCTAVE dan Kontrol 27001 pada Dishubkominfo Kabupaten Tulungagung," Semin. Nas. Sist. Inf. Indones., no. November, pp. 181–194, 2016.

G. M. Rahmah, "Analisis Manajemen Risiko Penerapan Sistem Informasi Di Politeknik Stmi Jakarta," J. Teknol. dan Manaj., vol. 17, no. 2, pp. 65–77, 2019.

J. Wijaya, A. Megafitri, K. Khotimah, R. Astriratma, S. Kom, and M. Cs, "Analisis dan Manajemen Risiko Keamanan Informasi pada Rumah Sakit Menggunakan Metode Octave Allegro (Studi Kasus: Rumah Sakit Umum Daerah Cengkareng)," Semin. Nas. Mhs. Ilmu Komput. dan Apl. Jakarta-Indonesia, no. September, pp. 762–774, 2021.

M. Z. Fathoni, "Analisis Risiko Pada Proyek Pembuatan Lintel Set Point Dengan Metode Kualitatif (Studi Kasus : PT. XYZ)," J. PASTI, vol. 14, no. 2, p. 113, 2020, doi: 10.22441/pasti.2020.v14i2.002.

R. W. Astuti, R. A. Putra, and I. S. Putra, "Penilaian Risiko Penggunaan Sistem Informasi Akademik Pada STIQ Al-Lathifiyyah Palembang Dengan Metode Octave Allegro," vol. 4, no. 1, pp. 44–54, 2023.

R. Ramadhintia and R. Bisma2, "Perencanaan Mitigasi Risiko Menggunakan Metode OCTAVE Allegro pada SMA Semen Gresik," J. Emerg. Inf. Syst. Bus. Intell., vol. 2, no. 2, pp. 17–23, 2021, [Online]. Available: https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/39087%0Ahttps://ejournal.unesa.ac.id

T. A. Bria, "Studi tentang Risiko yang Dihadapi Developer dalam Bisnis Properti," J. Univ. Atma Jaya Yogyakarta, vol. 5, no. 2, pp. 1–20, 2012.