Journal of Computer and Information Systems Ampera
Vol. 4, No. 1, January 2023 | e-ISSN: 2775-2496
10.51519/journalcisa.v4i1.337 | Published By APTIKOM SUMSEL

Penilaian Risiko Penggunaan Sistem Informasi Akademik Pada STIQ Al-Lathifiyyah Palembang Dengan Metode *Octave Allegro*

Riska Wini Astuti[1], Reza Ade Putra[2], Imamulhakim Syahid Putra[3]

[1]Sains dan Teknologi, Universitas Islam Negeri Raden Fatah, Palembang, Indonesia
[2,3]Sistem Informasi, Universitas Islam Negeri Raden Fatah, Palembang, Indonesia
Email: [1]ariskawini258@gmail.com, [2]rezaadepatra_uin@radenfatah.ac.id,
[3]imamulhakimsyahidputra_uin@radenfatah.ac.id

Abstrak

Penelitian ini dilakukan untuk mengevaluasi risiko yang dihadapi oleh sistem informasi akademik (SIAKAD) Sekolah Tinggi Ilmu Al-Quran (STIQ) Al-Lathifiyyah di kota Palembang. 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 kerangka risiko respons domain IT RISK (RR), 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 6 responden melalui observasi, wawancara, dan kuesioner. Hasil penelitian menunjukkan bahwa terdapat 5 ancaman risiko yang dihadapi oleh SIAKAD STIQ Al-Lathifiyyah, dengan 4 risiko yang memerlukan tindakan pengurangan risiko (mitigasi) dan 1 risiko yang dapat diterima dengan pendekatan tindakan yang sesuai (Accept). Penelitian ini diharapkan dapat memberikan informasi yang berguna bagi pengembangan SIAKAD dan pengelolaan risiko yang lebih efektif di STIQ Al-Lathifiyyah dan institusi serupa lainnya.

Kata Kunci: Sistem Informasi Akademik, Penilaian Risiko, Octave Allegro

1. PENDAHULUAN

Teknologi dimanfaatkan oleh lembaga atau organisasi untuk menunjang proses bisnis agar keberlangsungan sistem informasi tetap berjalan sebagaimana mestinya. Teknologi informasi merupakan komponen penting dalam mengelola sistem informasi, karena pengelolaan teknologi informasi juga merupakan salah satu aspek yang menentukan keberhasilan pelayanan perguruan tingggi tersebut. Sistem informasi adalah sistem yang ada dalam suatu organisasi dan diperlukan untuk mendukung transaksi organisasi sehari-hari, mendukung operasi, strategi dan operasi manajemen, dan menyediakan pelaporan yang diperlukan oleh pihak *eksternal* tertentu. Sistem informasi adalah kolaborasi perangkat keras, perangkat lunak, jaringan komunikasi, sumber daya, orang dan seperangkat kabijakan dan prosedur untuk memperoleh, memproses, mengarsipkan, mengubah, dan mendistribusikan informasi dalam suatu organisasi [1].

Sekolah Tinggi Ilmu Qur'an (STIQ) Al-Lathifiyyah merupakan perguruan tinggi Al-Qur'an di kota Palembang. Yang mana telah memanfaatkan teknologi informasi untuk mengelola data akademik yang sering dikenal dengan SIAKAD (Sistem Informasi Akademik) berbasis web. SIAKAD merupakan sistem informasi akademik pada Sekolah Tinggi Ilmu Qur'an Al-Lathifiyyah, SIAKAD ini pertama kali dibuat pada tahun 2018 dan memiliki beberapa fitur antara lain mulai dari pengambilan mata kuliah dan mencetaknya, melihat kartu hasil studi (KHS), mencari referensi buku, mencari ayat-ayat Al-Qur'an, 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 pihak staf dalam mengelola KRS, KHS dan lainnya kepada mahasiswa.

Sistem Informasi Akademik, banyak digunakan oleh hampir semua universitas khususnya di Indonesia, ini bertujuan untuk mempermudah pengiriman Informasi untuk siswa, 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[2]. 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 universitas [1]. Tujuan

Vol. 4, No. 1, January 2023 | e-ISSN: 2775-2496
https://journal-computing.org/index.php/journal-cisa/index

utama dari proses manajemen risiko adalah untuk melindungi organisasi sehingga dapat dengan maksimal dalam menjalankan visi dan misi organisasi, bukan hanya sekadar aset teknologi informasi saja. *Octave Allegro* merupakan salah satu metode manajemen risiko 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 mencapai misi dan tujuannya [3]. 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 [4]. Oleh karena itu kerangka kerja manajemen risiko yaitu *octave allegro*, salah satu kerangka kerja yang dibutuhkan dalam memanajemen risiko yang baik.

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[5]. Lukman Hakim Husnan, M.Ag selaku Kepala Pusat Teknologi Informasi (TI) pada STIQ Al-Lathifiyyah mengatakan, pada tahun 2021 STIQ Al-Lathifiyyah mengalami kebanjiran yang mengakibatkan ruang *server* yang terletak dilantai 1 terendam sedalam mata kaki, yang dikhawatirkan berdampak kerusakan pada *hardware* yang tentunya apabila terjadi kerusakan akan berdampak pula pada kegiatan SIAKAD, serta sebelumnya belum ada penelitian yang meneliti menegenai manajemen risiko khususnya penilaian risiko keamanan sistem informasi pada sistem informasi akademik STIQ Al-Lathifiyyah. Sehingga STIQ Al-Lathifiyyah belum mengetahui kemungkinan risiko dan tingkat risiko keamanan pada SIAKAD dan belum maksimal dalam persiapan untuk menanggulangi dampak dari risiko yang akan terjadi.

Dengan menerapkan manajemen risiko sistem informasi diharapkan dapat mengurangi dampak dari risiko yang akan terjadi, sehingga manajemen risiko sistem informasi sangat penting untuk diimplemetasikan pada STIQ Al-Lathifiyyah. Berdasarkan uraian

permasalahan diatas, maka peneliti melakukan penelitian Penilaian Risiko Pada Sistem Informasi Akademik STIQ Al-Lathifiyyah Menggunakan Metode Octave Allegro.

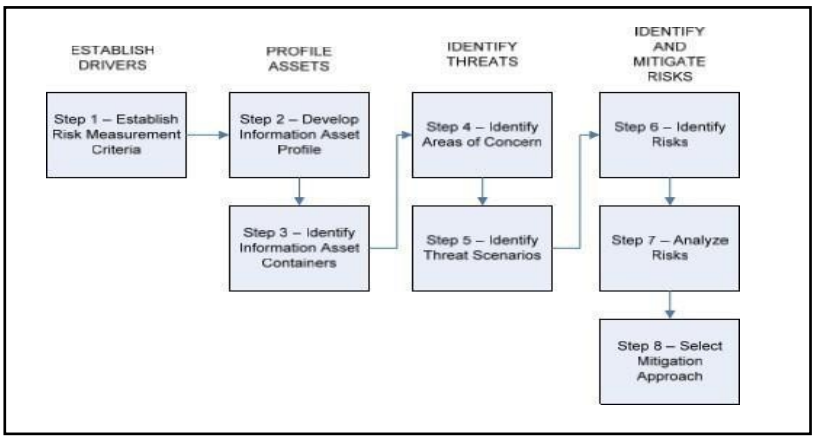
2. METODE

Penelitian ini menggunakan metode penelitian dan metode penilaian risiko. Metode penelitian menggunakan metode kualitatif dan untuk metode penilaian risiko menggunakan metode *Octave Allegro*.

2.1. Metode Penelitian

Penelitian ini menggunakan metode penelitian kualitatif dimana hasil dari penelitian ini disajikan dalam bentuk deskripsi. Penelitian ini dilakukan berdasarkan langkah-langkah pada metode *Octave Allegro,* dengan data yang diperoleh dari hasil wawancara langsung kepada narasumber di lapangan.

2.2. Metode Penilaian Risiko



Gambar 1. Langkah-langkah *OCTAVE Allegro* [6]

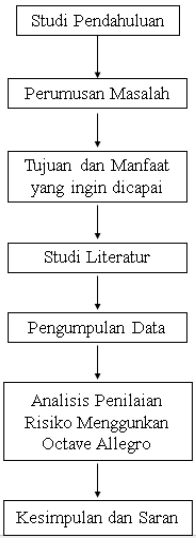
Metode penelitian penilaian risiko ini menggunakan metode *Octave Allegro*. *OCTAVE Allegro* merupakan sebuah *framework* yang menggunakan pendekatan *OCTAVE* dan didesain untuk melakukan penilaian risiko terhadap operasional organisasi atau perusahaan yang difokuskan pada asset informasi dengan tujuan untuk menghasilkan hasil yang lebih cepat tanpa memerlukan pengetahuan mendalam terkait

penilaian risiko. *Octave Allegro* dapat dilakukan dalam bentuk *workshop, setting* bersama yang didukung dengan panduan, lembar kerja, dan kuesioner, yang terdapat dalam lampiran *Octave Allegro*.

Pendekatan *OCTAVE Allegro* terdiri dari delapan langkah yang disusun dalam empat tahap, seperti yang diilustrasikan pada gambar diatas. Pada tahap 1, organisasi mengembangkan kriteria penilaian risiko yang konsisten dengan *driver* organisasi. Selama fase kedua, membuat profi aset dimana aset yang menjadi fokus penilaian risiko diidentifikasi dan digambarkan. Proses pembuatan profil ini menetapkan batasan yang jelas untuk aset tersebut, mengidentifikasi persyaratan keamanannya, dan mengidentifikasi semua lokasi penyimpanan, pengiriman, atau pemrosesan aset. Pada fase 3, ancaman terhadap aset informasi diidentifikasi dalam konteks lokasi penyimpanan, pengiriman, atau pemrosesan aset. Pada tahap akhir, risiko terhadap aset informasi diidentifikasi dan dianalisis dan pengembangan pendekatan mitigasi dimulai. Keluaran dari setiap langkah dalam proses ditangkap pada serangkaian lembar kerja yang kemudian digunakan sebagai masukan ke langkah berikutnya dalam proses.

2.3 Tahapan Penelitian

Tahapan penelitian yang akan dilakukan pada penelitian ini dapat dilihat pada Gambar 2.



Gambar 2.2. Tahapan Penelitian

3. HASIL DAN 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 1 Skala Prioritas Area Dampak

Lembar Kerja Allegro 7	LEMBAR KERJA PRIORITAS AREA DAMPAK
Prioritas	**Area Dampak**
5	Reputasi dan Kepercayaan Pengguna
4	Produktifitas
3	Keuangan
2	Keamanan dan Kesehatan
1	Denda dan Hukum

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 2 Profil Aset Informasi Kritis

Lembar Kerja Allegro 8	PROFIL ASET INFORMASI KRITIS	
(1) Aset Kritis Aset informasi apa yangkritis?	**(2) Alasan Untuk Seleksi** Mengapa aset informasi ini penting bagi organisasi?	**(3) Keterangan** Apa deskripsi yang disepakati pada aset informasi ini?
Aset Sistem Informasi Akademik	Karena apabila aset data informasi ini hilang dapat di salah gunakan, serta aset sistem informasi akademik berisikan data yang mendukungprosesutama dalam kegiatan operasionanl akademik STIQ AL-Lathifiyyah.	Aset informasi ini terdapat datamahasiswa (biodata, KRS, KHS, Transkrip Nilai), tugas, referensi, absensi, data dosen dan karyawan.
(4) Pemilik Siapa yangmemiliki aset informasi ini?		
Mahasiswa, Dosen, Admin Sistem Informasi, UPT. Pusat Data dan Teknologi Informasi		
(5) Persyaratan Keamanan Apa persyaratan keamanan untuk aset informasi ini?		

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 3. Peta Lingkungan Risiko Aset Informasi (Teknik)

Lembar Kerja Allegro 9a	**PETA LINGKUNGAN RISIKO ASET INFORMASI (TEKNIS)**
Internal	
Deskripsi Wadah	**Pemilik**
1. Module : Database layanan Sistem Informasi Akademik didalam *server* yang terdiri dari aset informasi akademik yang digunakan oleh Divisi IT, admin, dosen dan mahasiswa dalam menggunakan layanan	UPT. Pusat Data dan Teknologi Informasi
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	
Eksternal	
Deskripsi Wadah	**Pemilik**
Jaringan Internet : Menggunakan vendor pihak ketiga	Indihome
	My Republik

3.4 Mengidentifikasi *Area of Concern*

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

Tabel 4 *Areas Of Concern*

No	*Areas Of Concern*
1.	Ruangan *server* yang mudah diakses mengakibatkan *server* dapat diakses oleh pihak yang tidak berwenang (*hardware failure*)
2.	Pengeksploitasian celah keamanan sistem informasi akademik oleh pihak luar/dalam (*software failure*)
3.	*Server down* yang menyebabkan seluruh layanan tidak dapat berjalan/tidak dapat diakses (*hardware failure*)
4.	Terjadinya *bug/error* pada sistem saat pihak IT melakukan pengembangan dan pemeliharaan (*software flairue*)
5.	Terjadinya bencana alam yang mnyebabkan kerusakan pada perangkat-perangkat terkait dengan penunjang kegiatan sistem informasi (faktor alam)

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 5 Skenario Ancaman

	Area of Concern	*Threat of Properties*	
1.	Ruangan *server* yang mudah diakses mengakibatkan *server* dapat diakses oleh pihak yang tidak berwenang (*hardware failure*)	***Actors***	Tidak Diketahui
		Means	- *Password cracking* - *Rootkit*
		Motives	Secara disengaja
		Outcome	*Destruction, Disclosure, Interruption*
		Security Requirements	Hanya pihak yang berwenang yang dapat masuk kedalam ruang *server* dan mengakses serta memodifikasi *server*.
	Kemungkinan/ probabilitas	*Medium*	

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 6 Identifikasi Risiko

Skenario Ancaman	Konsekuensi
Ruangan *server* yang mudah diakses mengakibatkan *server* dapat diakses oleh pihak yang tidak berwenang (*hardware failure*)	Terjadinya kerusakan pada *server* dan penyalahgunaan hak akses oleh pihak yang tidak berwenang dan pencurian data penting

3.7 Menganalisis Risiko

Pada tahap ini, melakakun penilaian risiko relatif terhadap risiko yang telah ditentukan sebelumnya. Masing-masing risiko ditentukan skor penilaian terhadap area dampak (tinggi = 3, menengah = 2, rendah = 1)

Tabel 7 Analisis Risiko

Area Of Concern	*Risk*			
Ruangan *server* yang mudah diakses mengakibatkan *server* dapat diakses oleh pihak yang tidak berwenang (*hardware failure*)	***Consequences***	Terjadinya kerusakan pada *server* dan penyalahgunaan hak akses oleh pihak yang tidak berwenang dan pencurian data penting		
	Severity	***Impact Area***	***Value***	***Score***
		Reputasi dan Kepercayaan Pengguna	*High*	15
		Produktivitas	*High*	12
		Keuangan	*Medium*	6
		Kehidupan dan Keamanan	*High*	6
		Denda dan Hukum	*High*	3
		Relative Risk Score		42

3.7 Memilih Pendekatan Mitigasi

Pada tahap akhir ini, mengklasifikasikan setiap risiko yang telah diidentifikasi dan dianalisis dengan mempertimbangkan probabilitas dan skor relatifnya.

Tabel 8 *Relative Risk Matrix*

Relative Risk Matrix			
Probability	*Risk Score*		
	30 to 45	16 to 29	0 to 15
High	POOL 1	POOL 2	POOL 2
Medium	POOL 2	POOL 2	POOL 3
Low	POOL 3	POOL 3	POOL 4

Selanjutnya, menentukan pendekatan mitigasi yang sebelumnya telah diketahui dari tabel diatas untuk setiap risiko dengan berpedoman pada tabel pendekatan mitigasi yang dapat dilihat pada tabel berikut.

Tabel 9 Pendekatan Mitigasi

POOL	*Mitigation Approach*
POOL 1	*Mitigate*
POOL 2	*Mitigate or Defer*
POOL 3	*Defer of Accept*
POOL 4	*Accept*

Berikut ini adalah hasil akhir yang merupakan penentuan mitigasi yang ditentukan pada langkah sebelumnya, berikut risiko-risiko serta pendekatan mitigasi yang didapat:

Tabel 10 Penentuan Mitigasi

No	Risiko	*Relative Risk Score*	Probabilitas	POOL	Pendekatan Mitigasi
1.	Ruangan *server* yang mudah diakses mengakibatkan *server* dapat diakses oleh pihak yang tidak berwenang (*hardware failure*)	42	*Medium*	*POOL 2*	*Mitigate*
2.	Pengeksploitasian celah keamanan sistem informasi akademik oleh pihak luar/dalam (*software failure*)	32	*High*	*POOL 1*	*Mitigate*
3.	*Server down* yang menyebabkan seluruh layanan tidak dapat diakses (*hardware failure*)	19	*High*	*POOL 2*	*Mitigate*
4.	Terjadinya *bug/error* pada sistem saat pihak IT melakukan pengembangan dan pemeliharaan (*software flairue*)	30	*Medium*	*POOL 2*	*Mitigate*
5.	Terjadinya bencana alam yang menyebabkan kerusakan pada perangkat-perangkat terkait dengan penunjang kegiatan sistem informasi (faktor alam)	43	*Low*	*POOL 3*	*Accept*

4. KESIMPULAN

Berdasarkan hasil penilaian risiko yang dilakukan pada penelitian ini dapat disimpulkan bahwa penelitian dilakukan dengan metode *Octave Allegro* cocok untuk penilaian risiko. Penelitian ini menggunakan lima *impact areas* yaitu: reputasi dan kepercayaan pengguna, keuangan, produktivitas, keamanan dan kesehatan, serta denda dan hukum. Penelitian ini menunjukkan adanya 5 ancaman risiko. 4 risiko dengan pendekatan mitigasi yang harus dikurangi (*mitigate*) dan 1 risiko dengan pendekatan mitigasi yang dapat diterima (*Accept*).

DAFTAR PUSTAKA

[1] J. Hom, B. Anong, K. B. Rii, L. K. Choi, and K. Zelina, "Metode Oktaf Allegro dalam Manajemen Risiko Penilaian Institusi Pendidikan," no. 2, pp. 167–179, 2020.

[2] I. Kurniawan, I. Maita, and N. Yanti, "Pengukuran Risiko Sistem Informasi Perpustakaan Menggunakan Framework National Institute of Standard and Technology SP 800-30," pp. 270–277, 2020.

[3] N. L. Kuntari, Y. H. Chrisnanto, and A. I. Hadiana, "JENDERAL ACHMAD YANI MENGGUNAKAN METODA OCTAVE ALLEGRO," 2018.

[4] N. Ayu, N. Dewi, I. G. Putu, and H. Yudana, "ANALISA MANAJEMEN RISIKO PADA SISITEM AKADEMIK DI STMIK STIKOM BALI," pp. 6–7, 2016.

[5] Harsanto Kukuh, "MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY," vol. 6, no. 1, 2018.

[6] R. A. Caralli, "Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process," no. May, 2007.