Journal of Computer and Information Systems Ampera
Vol. 2, No. 1, January 2021 e-ISSN: **2775-2496**
https://journal-computing.org/index.php/journal-cisa/index

Analisis Penilaian Risiko Terhadap Penggunaan Sistem Informasi Akademik Pada Universitas Muhammadiyah Palembang Menggunakan Metode Octave Allegro

Kholifah[1], Reza Ade Putra[2], Fathiyah Nopriani[3]

[1]Sains dan Teknologi , Universitas Islam Raden Fatah, Palembang, Indonesia
[2,3]Sistem Informasi, Universitas Islam Negeri Raden Fatah, Palembang, Indonesia
Email: [1]kkholifah132@gmail.com, [2]rezaadepatra_uin@radenfatah.ac.id,
[3]fathiyahnopriani_uinradenfatah.ac.id

Abstract

The development of technology in meeting information needs has been implemented at the Muhammadiyah University of Palembang where there are various information systems used in managing information as a basis for creating quality services and supporting optimization in the work process. However, apart from the perceived benefits, the increasing dependence on information systems is in line with the risks that can arise, one of which is the risk of information security where information is an important asset for an organization that needs to be protected and secured. As an effort to maintain and protect information security, it is necessary to carry out risk evaluation in order to identify and anticipate risks that can interfere with information security. This study aims to conduct a risk assessment analysis of the use of Academic Information Systems as a very crucial information system in a university. This risk assessment analysis uses the Octave Allegro method with the main focus on information assets which consists of 8 steps and is organized into 4 stages starting with determining drivers, developing information asset profiles, identifying threats, and identifying and mitigating risks. The results of this study are 10 (ten) areas of concern with a mitigation approach of 7 (seven) risks that must be reduced (mittigate), 2 (two) risks that can be deferred (defer), and 1 (one) risk. that can be accepted (accept). From the risk assessment carried out, recommendations are given to prevent / minimize the identified risks as an effort to maintain and improve information security.

Keywords: Information Technology, Information Systems, Information Security, Assets, Risk Assessment, Octave Allegro.

Vol. 2, No. 1, January 2021 e-ISSN: **2775-2496**

https://journal-computing.org/index.php/journal-cisa/index

1. PENDAHULUAN

Teknologi informasi terus berkembang seiring kebutuhan layanan pendidikan yang semakin tinggi. Pelayanan yang baik menuntut perguruan tinggi berkolaborasi dengan teknologi untuk memberikan layanan terbaik. Pada saat ini telah banyak perguruan tinggi yang memanfaatkan teknologi dengan menitikberatkan pada penggunaan sistem informasi sebagai basis dalam penciptaan layanan yang berkualitas serta mendukung optimalisasi dalam proses kerjanya.

Salah satu Perguruan Tinggi Swasta di Sumatera Selatan yaitu Universitas Muhammadiyah Palembang (UMP) tengah bergerak maju dalam menerapkan teknologi dan sistem informasi. Dalam menunjang berkembangnya penerapan Teknologi Informasi (TI), UMP memiliki Unit Pelayanan Teknis (UPT) dalam bidang IT. Hingga saat ini telah banyak sistem informasi yang dikembangkan oleh UPT IT UMP diantaranya yaitu Sistem Informasi Penerimaan Mahasiswa Baru (SIPMB), Sistem Informasi Akademik (SIMAKAD), Sistem Informasi Dosen (SIMDOS), Sistem Informasi Kepegawaian (SIMPEG), Sistem Informasi Asset (SIMASET), Sistem Informasi Anggaran (SIM-ANGGARAN), Sistem Informasi Keuangan (SIMKEU), Sistem Informasi Terintigrasi (SISTER), Sistem Informasi Perpustakaan (e-Library), dan Career Development Center (CDC).

SIMAKAD merupakan sitem informasi yang sangat krusial bagi sebuah universitas dimana didalamnya terdapat data sebagai aset informasi kritis yang mendukung coreprocces dari universitas dalam menjalankan operasional akademik. Peranan sistem informasi akademik sangat penting karena merupakan pusat informasi yang menghubungkan antara civitas akademika, terutama pada mahasiswa dalam memperoleh informasi serta mengambil keputusan yang berhubungan dengan kegiatan akademik, seperti informasi nilai (krs), penentuan matakuliah (khs), informasi jadwal kuliah, bayaran, dan lain sebagainya.

Bagi Perguruan Tinggi, informasi dan teknologi yang mendukung kegiatan universitas merupakan aset yang berharga. Whitman dan Mattord dalam jurnal (Rosini, Rachmaniah dan Mustafa, 2015) mengungkapkan bahwa 'Data mempunyai peran yang sangat penting dalam sebuah sistem informasi karena merupakan salah satu komponen sistem informasi selain

software, hardware, people, procedures dan networks'. Perguruan Tinggi seringkali menggunakan sistem informasi dalam mengolah data yang kemudian diorganisir menjadi suatu informasi dan diterima sebagai pengetahuan serta digunakan untuk mengambil keputusan. Penggunaan sistem informasi mampu memberikan kemudahan dalam memenuhi kebutuhan informasi yang mendukung aktivitas pada sebuah organisasi. Namun, disamping memberi manfaat kemudahan, meningkatnya ketergantungan terhadap sistem informasi sejalan dengan risiko yang dapat ditimbulkan, salah satunya adalah risiko terhadap kemanan informasi dimana informasi merupakan aset penting bagi perguruan tinggi yang perlu dilindungi dan diamankan untuk menjamin ketersediaan informasi yang berguna dan dapat dipercaya baik oleh lingkungan internal maupun eksternal (Nugraha, 2016).

Berdasarkan hal tersebut, maka peneliti ingin melakukan kegiatan penilaian risiko untuk dapat mengetahui dan mengantisipasi risiko yang berpotensi dapat mengancam keamanan informasi dalam penggunaan sistem informasi. Penilaian risiko ini terutama diarahkan pada sistem informasi kritis yang mendukung coreproses atau aktivitas utama pada universitas seperti halnya Sistem Informasi Akademik.

2. METODE

Metode yang digunakan dalam penelitian ini yaitu metode penelitian dan metode penilaian risiko. Adapun metode penelitian yang digunakan adalah metode kualitatif dan untuk metode penilaian risiko yang digunakan adalah metode *Octave Allegro*.

2.1. Metode Penelitian

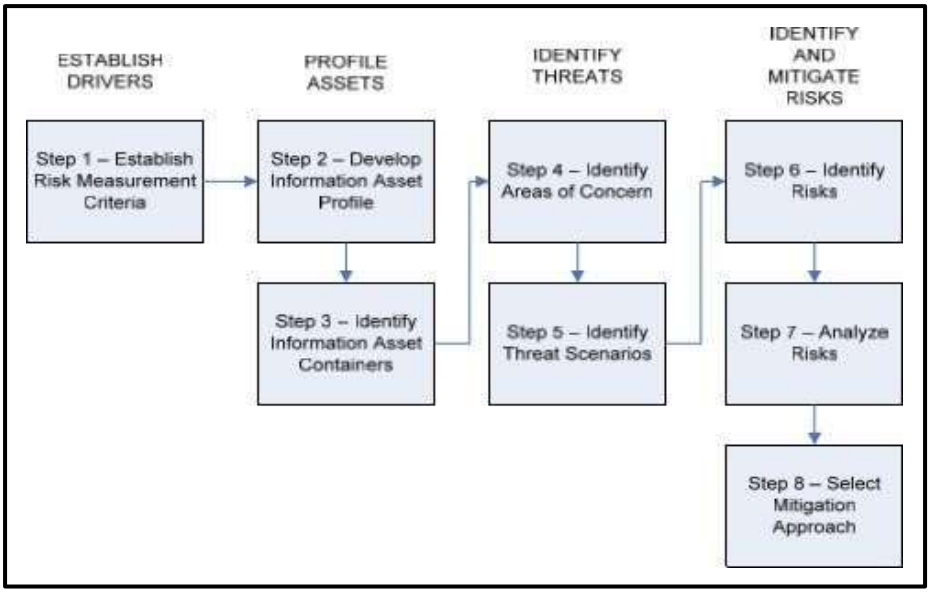
Metode penelitian yang digunakan adalah metode penelitian kualitatif dimana hasil dari penelitian dituangkan dalam bentuk deskripsi. Alasan penelitian ini menggunakan metode penelitian kualitatif karena sifat data atau hasil penelitian bercorak kualitatif, dimana penelitian ini menghasilkan data deskriptif yang didapat dari langkah-langkah yang ada pada metode *Octave Allegro* yang merupakan hasil dari pengetahuan atau pendapat narasumber setelah melakukan wawancara langsung di lapangan.

2.2. Metode Penilaian Risiko

Metode Penilain Risiko yang digunakan adalah *Octave Allegro*. *Octave Allegro* merupakan sebuah *framework* yang didesain untuk melakukan penilaian risiko terhadap operasional organisasi atau perusahaan yang difokuskan pada aset informasi dalam konteks bagaimana mereka digunakan, di mana mereka disimpan, diangkut, diproses dan bagaimana keadaannya jika terkena ancaman, kerentanan, dan gangguan sebagai hasil yang ditimbulkan.

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 2.1 berikut.



Sumber : Caralli, R. A. etc. 2007. Introducing OCTAVE Allegro :Improving the Information Security Risk Assessment Process.

Gambar 2.1. Langkah-langkah metode OCTAVE Allegro

Vol. 2, No. 1, January 2021 e-ISSN: 2775-2496

https://journal-computing.org/index.php/journal-cisa/index

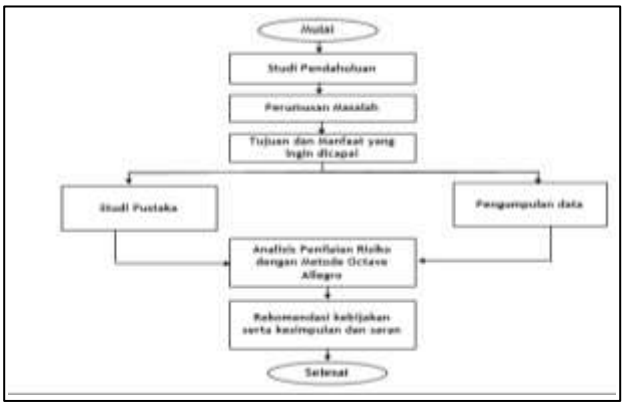
Dari gambar tersebut dapat dijelaskan bahwa metode *octave allegro* terdiri dari 8 langkah yang disusun dalam 4 tahap sebagai berikut :

- Fase 1 : Menetapkan Driver
  Langkah 1. membangun kriteria pengukuran risiko
- Fase 2 : Mengembangkan Profil Aset
  Langkah 2. mengembangkan profil aset informasi
  Langkah 3. mengidentifikasi kontainer aset informasi
- Fase 3 : Identifikasi Ancaman
  Langkah 4. mengidentifikasi area ancaman
  Langkah 5. mengidentifikasi skenario ancaman
- Fase 4 : Identifikasi dan Mitigasi Risiko
  Langkah 6. mengidentifikasi risiko
  Langkah 7. menganalisis risiko
  Langkah 8. menentukan pendekatan mitigasi

Keluaran dari setiap langkah dalam proses penilaian risiko ditangkap pada serangkaian lembar kerja yang kemudian digunakan sebagai masukan ke langkah berikutnya. Pada lembar kerja ini, informasi ancaman dan dampak yang terkait dengan risiko ditangkap, skor risiko relatif dihitung, rencana dan kegiatan mitigasi didokumentasikan. Hal ini secara signifikan dapat mengurangi manipulasi dokumentasi, organisasi, dan data yang diperlukan untuk melakukan penilaian risiko serta menghasilkan pandangan risiko yang jauh lebih ringkas.

2.3. Tahapan Penelitian

Tahapan Penelitian menggambarkan proses penelitian yang akan ditempuh sekaligus menggambarkan penelitian secara keseluruhan. Tahapan penelitian dapat dilihat pada Gambar 2.2 berikut.



Gambar 2.2. Tahapan Penelitian

3. HASIL DAN PEMBAHASAN

Penelitian ini menerapkan seluruh tahapan yang ada pada *Octave Allegro* dengan menggunakan paduan lembar kerja yang telah disediakan pada *Octave Allegro*. Berikut hasil dari langkah-langkah *Octave Allegro*:

1. Membangun Kriteria Pengukuran Risiko
   Dengan menggunakan paduan lembar kerja 1, terdapat dua aktivitas yang dilakukan diawali dengan menentukan kriteria pengukuran risiko kemudian memprioritaskannya. Hasil dari langkah 1 dapat dilihat pada tabel berikut.

Tabel 3.1 Kriteria Pengukuran Risiko

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

2. Mengembangkan Profil Aset Informasi
   Langkah ini fokus pada menentukan dan mengumpulkan informasi mengenai aset informasi yang terdapat pada sistem informasi akademik untuk dilakukan proses penilaian risiko terstruktur dengan menggunakan lembar kerja 8 sebagai berikut.

Tabel 3.2 Kriteria Pengukuran Risiko

Lembar Kerja Allegro 8	**INFORMASI AKTIVA INFORMASI KRITIS**	
(1) Aset Kritis Aset informasi apa yang kritis?	**(1) Alasan Untuk Seleksi** Mengapa aset informasi ini Penting bagi organisasi?	**(3) Keterangan** Apa deskripsi yang disepakati pada aset informasi ini?
Aset informasi dalam Sistem Informasi Akademik	Aset informasi ini berisikan data/informasi penting mengenai kegiatan akademik yang mendukung *coreproses* UMP dalam menjakankan aktivitas utamanya yaitu melaksankan operasional akademik.	Aset informasi akademik terdiri dari : 1. Data Mahasiswa, meliputi biodata diri, KRS online, KRS Semester, KHS Semester, dan Transkrip Nilai 2. Data Pembayaran, meliputi Cek Tagihan Pembayaran UKT dan Riwayat Pembayaran UKT 3. Jadwal Kuliah dan Kurikulum, meliputi Jadwal Kuliah dan kurikulum
(4) Pemilik Siapa yang memiliki aset informasi ini?		
Divisi IT, Admin Sistem Informasi, Dosen, BAAK dan Mahasiswa		

(5) Persyaratan Keamanan Apa persyaratan keamanan untuk aset informasi ini?		
Kerahasiaan	Memastikan bahwa hanya orang yang berwenang yang memiliki akses ke informasi	Data/ informasi akademik hanya dapat diakases oleh admin, dosen dan mahasiswa dengan domain dan halaman akses yang berbeda sesuai dengan ketentuan yang telah ditetapkan (*Acces Previlage Management*).
Integritas	Memastikan bahwa asset informasi tetap dalam kondisi yang dimaksudkan oleh pemilik dan untuk tujuan yang dimaksudkan oleh pemiliknya.	Informasi harus benar dan akurat dan hanya pihak berwenang yang dapat memodifikasi aset informasi, seperti : 1. Dosen hanya dapat menginput nilai untuk khs mahasiswa melalui halaman dosen 2. Admin dapat menambahkan jadwal dan matakuliah serta mengubah data apabila terjadi kesalahan oleh mahasiswa dan dosen melalui halaman admin 3. Divisi IT sebagai pusat pengelola sistem informasi yang dapat mengakses secara keseluruhan apabila diharuskan.
Ketersediaan	Memastikan bahwa aset informasi tetap dapat diakses oleh pengguna yang berwenang	Aset infromasi ini dapat diakses dalam waktu 7x24 jam selama tidak terjadi *trouble* yang diluar dugaan.
(6) Persyaratan keamanan yang paling penting Apa persyaratan keamanan terpenting untuk aset informasi ini?		
Kerahasiaan	✓ Integritas	Tersediannya

3. Mengidentifikasi Kontainer Aset Informasi

Tahapan ini menjelaskan tentang identifikasi kontainer aset informasi yang merupakan tempat dimana aset informasi tersebut disimpan, dipindahkan, dan diproses. Kontainer aset informasi meliputi aspek *technical, physical, dan people* yang didokumentasikan pada lembar kerja 9.

Tabel 3.3 Peta Lingkungan Risiko Aset Informasi (Teknik)

Lembar Kerja Allegro 9a	**PETA LINGKUNGAN RISIKO ASET INFORMASI (TEKNIK)**
Internal	
Deskripsi Kontainer	**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	Universitas (UPT IT)
2. Server : digunakan sebagai media penyimpanan aplikasi dan database dengan menggunakan jaringan internet	Universitas (UPT IT)
3. Perangkat jaringan : kabel *Fiber Optic, Terminal, router, switch/hub*, dan *acces point*	Universitas (UPT IT)
4. Jaringan Internet Internal : LAN	Universitas (UPT IT)

5. Komputer : perangkat komputer server	Universitas (UPT IT)
6. Sistem Operasi server : Linux dan windows server	Universitas (UPT IT)
7. Aplikasi : Sistem Informasi Akademik , Aplikasi Keuangan	Universitas (UPT IT, Admin, Dosen, Mahasiswa)
Eksternal	
1. Jaringan Internet : Menggunakan vendor pihak ketiga	- Telkom
	- Moratelindo
2. Server Eksternal : digunakan sebagai *back-up* dari server pusat	Datacenter Moratelindo

4. Mengidentifikasi *Area Of Concern*
   Mengidentifikasi *Area of Concern* dalam langkah ini yaitu dengan membuat pernyataan deskriptif yang menjabarkan kondisi atau situasi yang dapat mempengaruhi aset informasi dengan meninjau kembali setiap kontainer yang telah ditentukan sebagai sumber dari risiko yang teridentifikasi serta studi pustaka yang merujuk pada literatur manajemen risiko dan keamanan informasi untuk melihat dan menentukan areas of concern yang potensial.

Tabel 3.4 *Area Of Concern*

No	*Area Of Concern*
1	Ruangan server yang mudah diakses mengakibatkan server dapat diakses oleh pihak yang tidak berwenang *(hardware failure)*
2	*Server down* yang menyebabkan seluruh layanan tidak dapat berjalan/tidak dapat diakses *(hardware failure)*
3	Sistem tidak dapat diakses karena terdapat gangguan jaringan *(network failure)*
4	Pengeksploitasian celah kemananan sistem informasi akademik oleh pihak dalam/luar *(software failure)*
5	Kesalahan dalam input data/informasi akademik oleh admin dan dosen *(human error)*
6	Bocornya hak akses seperti *username* dan *password (human error)*
7	Laporan Pembayaran UKT yang tidak valid (*software failure*)
8	Terjadinya *bug/error* pada sistem saat pihak IT melakukan pengembangan dan pemeliharaan *(software flairue)*
9	Berhentinya layanan sistem informasi akademik dikarenakan *supply* listrik mati *(power failure)*
10	Terjadinya bencana alam yang menyebabkan kerusakan pada perangkat-perangkat terkait dengan penyediaan sistem informasi (faktor alam)

5. Mengidentifikasi Skenario Ancaman
   Pada tahap ini akan dilakukan identifikasi skenario ancaman (threat scenario) dengan memberikan gambaran secara rinci mengenai properti dari ancaman antara lain *actor, means, motives, outcome* dan *security* untuk setiap *area of concern*.

Tabel 3.5 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 Sengaja
		Outcome	*Destruction, Disclosure, Interruption*
		Security Requirements	Hanya pihak yang berwenang yang dapat masuk kedalam ruang *server* dan mengakses serta memodifikasi *server*.
	Kemungkinan/ Probabilitas	*Low*	

6. Mengidentifikasi Risiko
   Aktivitas yang dilakukan pada tahap ini adalah menentukan bagaimana *threat scenario* yang telah ditentukan dapat memberikan dampak bagi organisasi dimana untuk setiap skenario yang telah dibuat, harus ditentukan dampak/konsekuensi yang mungkin akan ditimbulkan ketika ancaman terjadi dan didokumentasikan pada lembar kerja risiko aset informasi (lembar kerja 10) bagian ke-7.

Tabel 3.6 Skenario Ancaman

Skenario Ancaman	**Konsekuensi**
Ruangan server yang mudah diakses mengakibatkan server dapat diakses oleh pihak yang tidak berwenang *(hardware failure)*	- Merusak perangkat sehingga menyebabkan kerusakan pada server - Terjadinya penyalahgunaan hak akses oleh pihak yang tidak berwenang dan pencurian data penting - Pencurian perangkat dalam ruangan server

7. Analisis Risiko
   Pada langkah ini aktivitas yang dilakukan yaitu melakukan analisis risiko dengan mengevaluasi konsekuensi dari risiko terhadap organisasi dengan memperimbangkan kriteria pengukuran risiko yang diciptakan pada langkah 1 aktivitas 1. Dilanjutkan dengan menghitung skor dampak area dan skor risiko relatif pada setiap risiko aset informasi. Dalam hal ini penentuan *score* diperoleh melalui perkalian prioritas area dampak yang terdapat pada langkah 1 aktivitas 2 dengan *value* dari impact area yang ditetapkan dalam *octave allegro* dibagi

kedalam tiga kategori yaitu : *High=3, medium=2, dan low=1*. Sedangkan skor risiko relatif merupakan skor risiko total yang telah dihitung sebelumnya, dapat dilihat pada tabel berikut.

Tabel 3.7 Penentuan Skor *Impact Area*

Area Dampak	Prioritas	Skor Dampak		
		Rendah (n= (1))	Sedang (n= (2))	Tinggi (n= (3))
Produktivitas	5	5	10	15
Reputasi dan Kepercayaan Pengguna	4	4	8	12
Keuangan	3	3	6	9
Keamanan dan Kesehatan	2	2	4	6
Denda dan Hukum	1	1	2	3

Tabel tersebut digunakan untuk menentukan skor dari area dampak yang kemudian dilanjutkan dengan menghitung skor risiko relatif. Untuk hasil analisis risiko.

Tabel 3.7 Analisis Risiko

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

8. Analisis Risiko
   Aktivitas pertama yang dilakukan pada langkah ini adalah mengklasifikasikan setiap risiko yang telah diidentifikasi dan dianalisis dengan mempertimbangkan probalilitas dan skor risiko relatifnya. Pengklasifikasian menggunakan acuan *relative risk matrix* yang dapat dilihat pada tabel berikut.

Tabel 3.8 Tabel *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

Aktivitas selanjutnya adalah 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 3.9 Tabel *Mitigation Approach*

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

Untuk hasil dari penentuan mitigasi dapat dilihat pada tabel dibawah ini sekaligus sebagai hasil akhir dari perhitungan penilaian risiko yang kemudian dilanjutkan dengan pemberian rekomendasi atau solusi dari risiko yang telah dianalisis.

Tabel 3.10 Tabel 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	*Low*	*Pool 3*	*Defer*
2	*Server down* yang menyebabkan seluruh layanan tidak dapat berjalan/tidak dapat diakses *(hardware failure)*	20	*High*	*Pool 2*	*Mitigate*
3	Sistem tidak dapat diakses karena terdapat gangguan jaringan *(Network Failure)*	20	*Medium*	*Pool 2*	*Mitigate*
4	Pengeksploitasian celah kemananan sistem informasi akademik oleh pihak dalam/luar *(Software Failure)*	33	*High*	*Pool 1*	*Mitigate*
5	Kesalahan dalam input data/informasi akademik *(human error)*	24	*Medium*	*Pool 2*	*Mitigate*

6	Bocornya hak akses seperti username dan password *(human error)*	**21**	***Medium***	***Pool 2***	***Mitigate***
7	Laporan Pembayaran UKT yang tidak valid	**30**	***Low***	***Pool 3***	***Defer***
8	Terjadinya bug/error pada sistem saat pihak IT melakukan pengembangan dan pemeliharaan *(software flairue)*	**31**	***Medium***	***Pool 2***	***Mitigate***
9	Berhentinya layanan sistem informasi akademik dikarenakan *supply* listrik mati *(power failure)*	**20**	***Medium***	***Pool 2***	***Mitigate***
10	Terjadinya bencana alam yang menyebabkan kerusakan pada perangkat-perangkat terkait dengan penyediaan sistem informasi (faktor alam)	**43**	***Low***	***Pool 3***	***Accept***

Setelah menyelesaikan serangkaian proses penilaian risiko, selanjutnya akan diberikan rekomendasi untuk memitigasi risiko sebagai berikut.

1. Ruangan *server* yang mudah diakses mengakibatkan *server* dapat diaskes oleh pihak yang tidak berwenang
   - Memastikan agar pintu ruangan server terkunci dengan aman dan hanya pihak yang berwenang yang dapat masuk atau bila memungkinkan, memasang *doorlock* yang menggunakan *fingerprint, face recognition* maupun *access code* (Elanda dan Tjahjadi, 2018).
   - *Mendisable* (menutup) port yang tidak dibutuhkan, sehingga tidak bisa menggunakan sembarang *port* untuk melakukan *copy* data (Aristasari dan Riadi, 2011).
2. *Server down* yang menyebabkan seluruh layanan tidak dapat berjalan/tidak dapat diakses
   - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin sehingga perangkat terhindar dari risiko akibat *overheat* (Rilyani, Firdaus dan Jatmiko, 2015).
   - Menyesuaikan kapasitas dengan jumlah user serta menghilangkan log yang menggunakan kapasitas besar untuk mengatasi *overcapacity* dan *overload* (Rilyani, Firdaus dan Jatmiko, 2015).
   - Melakukan *restart database service* (Rilyani, Firdaus dan Jatmiko, 2015).
   - Mengecek koneksi internet dan rutin menghapus *cache* dan *cookies* (Thenu, Wijaya dan Rudianto, 2020).

Vol. 2, No. 1, January 2021 e-ISSN: **2775-2496**

https://journal-computing.org/index.php/journal-cisa/index

3. Sistem tidak dapat diakses karena terdapat gangguan jaringan *(Network flairue)*
   - perlunya melakukan tindakan control jaringan dengan cara dimonitoring dan dipelihara keamanan sistemnya yang ditinjau secara berkala (Mahersmi, Artowini dan Hidayanto, 2016)
4. Pengeksploitsian celah keamanan sistem informasi akademik oleh pihak dalam/luar *(software failure)*
   - Melakukan *update patching* secara berkala pada *software* dan sistem operasi (Aristasari dan Riadi, 2011).
   - *Instalasi firewall*, antivirus serta melakukan modifikasi default *security system* (Nurochman, 2014).
5. Kesalahan dalam melakukan input data/informasi akademik oleh admin maupun dosen
   - Melakukan pengecekan ulang sebelum data di inputkan dalam sistem oleh dosen dan admin.
   - Mahasiswa segera melaporkan kepada dosen/admin apabila terjadi kesalahan dalam informasi yang diterima.
   - Membuat suatu validasi perbaikan untuk mengecek data yang tidak sesuai dan *control* pada sistem untuk pengecekkan data yang sama dengan memberikan suatu identifikasi bahwa data yang diinputkan telah ada (Dewi dan Yudana, 2016).
6. Bocornya hak akses seperti *username* dan *password (human error)*
   - Melakukan perubahan *password* secara berkala (Nurochman, 2014).
   - Memberikan penyuluhan untuk menjaga kerahasiaan hak akses untuk menghindari terjadinya risiko bocornya hak akses dan terjadinya penyalahgunaan hak akses (Safar, 2019).
7. Laporan Pembayaran UKT yang tidak valid
   - Membuat SOP untuk kasus-kasus khusus (Pujastuti dan Naisiri, 2016).
   - Melakukan pengecekan kembali hasil laporan pada aplikasi keuangan dengan laporan dari bank (Pujastuti dan Naisiri, 2016).
8. Terjadinya *Bug/error* pada sistem saat pihak IT melakukan pengembangan dan pemeliharaan *(software failure)*
   - melakukan pengujian terhadap perangkat lunak dan jaminan kualitas perangkat lunak (Budiarto, 2017).

9. Berhentinya layanan sistem informasi akademik dikarenakan *supply* listrik mati *(power failure)*
   - melakukan perbaikan dan penambahan kapasitas genzet serta penggunaan UPS (uninterterrupted power supply) sehingga layanan sistem informasi tidak berhenti dan aktivitas kampus dapat tetap berjalan sampai supply listrik kembali normal (Nurochman, 2012).
10. Terjadinya bencana alam yang menyebabkan kerusakan pada perangkat-perangkat terkait dengan penyediaan sistem informasi (faktor alam).
    - melakukan tindakan perlindungan keamanan pengkabelan dari kerusakan untuk menghindari terjadinya risiko kebakaran yang disebabkan karena *korsleting* listrik dan terbakarnya generator baik di ruangan server maupun ruang lainnya yang terkoneksi dengan kabel (Mahersmi, Artowini dan Hidayanto, 2016).

4. KESIMPULAN

Universitas Muhammadiyah palembang belum pernah melakukan evaluasi risiko terhadap penggunaan sistem informasi yang berjalan. Oleh karena itu, dilakukan penilaian risiko pada penelitian ini dimana penilaian risiko ini dilakukan pada sistem informasi akademik sebagai sistem informasi yang sangat krusial bagi sebuah universitas sehingga penilaian risiko pada sistem ini diprioritaskan terlebih dahulu. Metode yang digunakan adalah metode octave allegro dengan fokus pada aset informasi yang teridiri dari 8 langkah dan disusun dalam 4 tahap.

Dari penelitian yang telah dilakukan menghasilkan 10 area of concern dengan strategi pengurangan risiko menghasilkan mitigate berjumlah 7, defer berjumlah 2, dan accept berjumlah 1. Dari hasil penilaian risiko, peneliti memberikan rekomendasi untuk dapat mencegah atau meminimalisir risiko yang berhasil diidentifikasi dengan menerapkan langkah yang terdapat pada octave allegro dan mempelajari literatur terkait manajemen risiko terhadap keamanan informasi.

DAFTAR PUSTAKA

[1] Aristasari, P. dan Riadi, I. (2011) “Manajemen Risiko Pada Learning Management System Menggunakan Kerangka Kerja OCTAVE Allegro,” hal. 1–15.

[2] Budiarto, R. (2017) "Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode Fmea Dan Iso 27001 Pada Organisasi Xyz," *Journal of Computer Engineering System and Science*, 2(2), hal. 105–115. doi: 10.24114/cess.v2i2.6264.

[3] Caralli, R. A. *et al.* (2007) "Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process," (May).

[4] Dalafranka, M. L., Syamsuar, D. dan Novaria, Y. (2018) "Information Technology Risk Assessment Sistem Informasi Elektronik Kinerja Pegawai Universitas Islam Negeri," *Seminar Nasional Teknologi Informasi Dan Komunikasi (SEMNASTIK) X*, hal. 153–158.

[5] Darmawi, H. (2006) *Manajemen Risiko*. Jakarta: Bumi Aksara.

[6] Destrianto, F. R., Nelmiawati dan Sitorus, M. A. (2017) "Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE," *Jurnal Integrasi*, 9(1), hal. 35–47.

[7] Dewi, N. A. N. dan Yudana, I. G. P. H. (2016) "Analisa Manajemen Risiko Pada Sistem Akademik di STMIK STIKOM Bali," *Seminar Nasional Teknologi Informasi dan Multimedia 2016*, 1, hal. 1.5.7-1.5.12.

[8] Gondodiyoto, S. (2007) *Audit sistem Informasi Pendekatan COBIT*. Jakarta: Penerbit Mitra Wacana.

[9] Hendarti, H. dan Maryani (2014) "DENGAN METODE OCTTAVE-S," 5(9), hal. 917–924.

[10] Idroes, F. N. (2008) *Manajemen Risiko Perbankan: Pemahaman Pendekatan 3 Pilar Kesepakatan Bassel II Terkait Aplikasi Regulasi dan Pelaksanaannya di Indonesia*. Jakarta: Rajawali Pers.

[11] Jakaria, D. A., Dirgahayu, R. T. dan Hendrik (2013) "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro," *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, hal. E-37-E42.

[12] Krutz, R. L. dan Vines, R. l D. (2006) *The CISSP Prep Guide - Mastering the Ten Domains of Computer Security*. Wiley Computer Publishing John Wiley & Sons, Inc.