

## MANAJEMEN RISIKO SISTEM INFORMASI DI UNIVERSITAS JENDERAL ACHMAD YANI MENGGUNAKAN METODA OCTAVE ALLEGRO

**Niken Laras Kuntari<sup>1\*</sup>, Yulison Herry Chrisnanto<sup>2</sup>, Asep Id Hadiana<sup>3</sup>**

*Jurusan Informatika, Fakultas Sains dan Informatika (FSI)*

*Universitas Jenderal Achmad Yani*

*Jl. Terusan Jenderal Sudirman Cimahi*

*Email: Nikenlaras324@yahoo.co.id<sup>1</sup>*

*Jurusan Informatika, Fakultas Sains dan Informatika (FSI)*

*Email: y.chrisnanto@gmail.com<sup>2</sup>*

*Jurusan Informatika, Fakultas Sains dan Informatika (FSI)*

*Email : ahadiana@gmail.com<sup>3</sup>*

### ABSTRAK

Dalam rangka meningkatkan kemampuan Unjani dalam melaksanakan tugas kependidikan diperlukan dukungan secara teknis dari teknologi informasi sehingga ada sejumlah investasi yang dilakukan guna tersedianya teknologi informasi sebagai penopang aktivitas organisasi. Investasi yang telah dilakukan merupakan *asset* penting yang perlu dipelihara. Banyak peristiwa yang terjadi pada kurun waktu tertentu yang dapat mengancam keberadaan *asset* tersebut antara lain, bencana alam, kebakaran, huru hara, kejahatan siber dan lain sebagainya. Resiko atas ancaman tersebut harus dapat dikelola sedemikian sehingga dampak atas resiko tersebut dapat diminimalisir. Pada penelitian ini *metoda Octave Allegro* digunakan untuk menilai besar ancaman dari sebuah resiko khususnya terkait dengan *asset* teknologi informasi yang dimiliki Unjani. Dalam *Octave Allegro* terdapat 8 aspek yang perlu dinilai dimana aspek tersebut diselesaikan dalam 4 fase, dengan jumlah responden sebanyak 21 orang sebagai pemakai teknologi informasi serta 3 orang pengelola teknologi informasi di Unjani. Hasil penelitian ini menunjukkan bahwa *asset* teknologi informasi yang ada di Unjani memiliki resiko yang tinggi yang berdampak pada keberlangsungan pemanfaatan IT tersebut. Hal tersebut dikarenakan tata kelola IT belum dilakukan secara konstruktif. *Octave Allegro* dapat memperlihatkan resiko yang mungkin muncul atas dampak dari ancaman.

***Kata kunci: asset, teknologi informasi, risiko, Metoda Octave Allegro, mitigasi***

### PENDAHULUAN

Teknologi Informasi (TI) telah banyak diterapkan pada institusi pendidikan atau organisasi pendidikan. Organisasi yang baik mengetahui bahwa TI dapat meningkatkan nilai dalam aktivitas utama dan aktivitas pendukung. TI akan bermanfaat jika penerapannya sesuai dengan visi dan misi organisasi. Jika keberadaan TI tidak dimanfaatkan dengan baik maka akan mengakibatkan berbagai permasalahan seperti keamanan data terganggu, kebocoran data, kerugian organisasi karena TI yang diterapkan tidak dapat menunjang aktivitas organisasi, dan sebagainya.

Pada saat ini banyak perguruan tinggi telah memanfaatkan teknologi *web* sebagai sarana untuk melayani mahasiswa dalam bidang akademik. Sifat teknologi *web* yang mudah diakses dan digunakan menjadi alasan utama beberapa perguruan tinggi memilihnya untuk pelayanan akademik. Penelitian ini akan mengamati layanan akademik berbasis *web* pada salah satu perguruan tinggi penelitian ini memfokuskan pada identifikasi, analisis dan penilaian risiko Sistem Informasi Akademik berbasis *web* pada perguruan tinggi menggunakan *metoda Octave Allegro* [1]

*Metode Octave Allegro* adalah kerangka kerja penilaian risiko TI di perguruan tinggi dengan hasil berupa dokumentasi berupa profil risiko yang dapat mengancam keberlangsungan sistem informasi dan solusi pencegahan melalui rekomendasi kontrol sebagai tindak lanjut proses berikutnya melalui kegiatan mitigasi risiko. Oleh karena itu untuk mendefinisikan risik dan meminimalisir risiko yang mungkin terjadi dan



memberikan saran penanggulangan yang tepat maka perlu diadakannya manajemen risiko pada teknologi informasi di Universitas Jenderal Achmad Yani.

### **Rumusan Masalah**

Unjani pernah mengalami kehilangan data akademik yang mengakibatkan terhambatnya penyaluran informasi antara data yang tersimpan di dalam basis data kepada pengguna sistem informasi akademik, hal tersebut berarti bahwa tata kelola TI belum dilakukan dengan baik. Pengaksesan salah satu sistem informasi Unjani juga belum sesuai dengan target yang ditetapkan pada dokumen rencana strategis (renstra) sehingga hal tersebut berarti bahwa terdapat beberapa poin renstra yang belum sesuai dengan implementasinya serta adanya kontrol yang belum maksimal pada penerapan TI di organisasi.

Dalam kegagalan teknologi informasi belum ada pengukuran sistem sehingga dampak risiko terkadang belum ada pencegahan dalam mengelola risiko itu sendiri dan diperlukan upaya secara terukur dan belum ada kebijakan dalam pengelolaan sistem itu sendiri. Sehingga pihak manajemen menemukan kesulitan dalam menjaga sistem dan menemukan pentingnya peran sistem dalam setiap fungsi asset-aset informasi.

### **Penelitian terdahulu**

Pada penelitian yang telah dilakukan yaitu manajemen risiko sistem informasi akademik pada perguruan tinggi menggunakan *metoda octave allegro*. Tujuan dari penelitian ini adalah untuk mengidentifikasi, menganalisis dan mengelola risiko sistem informasi akademik pada perguruan tinggi metode *octave allegro*. Mengembangkan strategi keamanan sistem informasi untuk meningkatkan keamanan sistem informasi. Hasil dari penelitian maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritical secara tepat serta langkah-langkah pemulihan jika skenario ancaman benar-benar terjadi. (Deni Ahmad Zakaria, 2013)

Pada penelitian yang telah dilakukan yaitu analisis manajemen risiko untuk evaluasi aset menggunakan metode *octave allegro*. Menjelaskan bahwa aset merupakan aset merupakan sumber daya yang dimiliki untuk dapat melakukan operasi dalam suatu perusahaan yang kemudian dapat memberikan manfaat usaha di kemudian hari. Serta dalam penilaian aset hasil penilaian risiko 7 dengan nilai tinggi dan 1 nilai sedang. Dengan menerapkan manajemen risiko pihak manajemen dapat mengetahui dampak ancaman, kerawanan dan akibat dari masing-masing aset yang ada. (Joshua Jenriwan L Tobing, 2015)

Metode *octave allegro* memberikan panduan secara sistemik dan komprehensif. Dalam manajemen risiko keamanan informasi. Metode ini lebih menekankan pengelolaan risiko berbasis ancaman, dan kelemahan terhadap aset-aset informasi organisasi meliputi perangkat keras, lunak, sistem, informasi dan manusia. (Supradono, 2009)

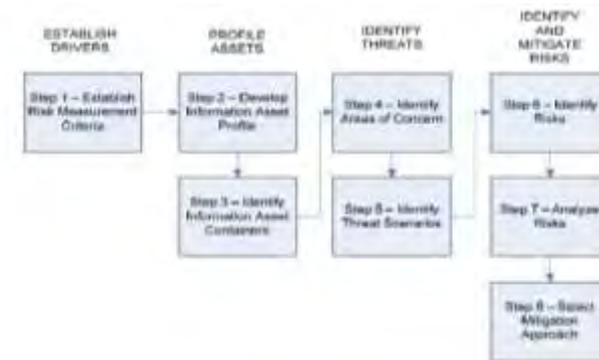
Pada penelitian yang telah dilakukan yaitu Manajemen Risiko Aplikasi Pembelajaran Berbasis *Online* Pada Universitas Dengan Menggunakan Metode *Octave Allegro*. Penelitian ini menjelaskan bahwa keberlangsungan proses bisnis dapat terganggu jika aplikasi pembelajaran *online* ini mengalami suatu gangguan baik karena kesalahan teknis, kesalahan perangkat keras, kesalahan di dalam penulisan sintak perangkat lunak, kesalahan logika, gangguan lingkungan, kegagalan arus listrik karena petir dan kesalahan manusia. *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. (Henki Bayu Seta, 2017)

### **Pembahasan**

#### **1. Metodologi penelitian**

*Octave allegro* merupakan seperangkat peralatan, teknik dan metode untuk penilaian perencanaan keamanan sistem informasi berbasis risiko. *Octave Allegro* memfokuskan pada aset informasi data dan data yang mendukung informasi tersebut. *Octave Allegro* terdiri dari 8 langkah dan dibagi menjadi 4 fase. Perhatikan Gambar 1 berikut ini.





**Gambar 1 Langkah Langkah *Octave Allegro* (Richard A. Caralli, May 2007)**

Tahapan penilaian risiko

Dalam metode *Octave Allegro* terdapat 8 langkah yakni sebagai berikut:

- a. Membangun Kriteria Pengukuran Risiko  
Langkah ini terdapat dua aktivitas, diawali dengan membangun *organizational drivers* digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali *impact area* yang paling penting. Aktivitas 1 yaitu membuat definisi ukuran kualitatif yang di dokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas dua melakukan pemberian nilai prioritas pada *impact area* menggunakan *impact area ranking worksheet*.
- b. 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 informasi aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deksripsi aset informasi kritis tersebut. Aktivitas tujuh mengisi keamanan untuk *confidentiality*, *integrity* dan *availability*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untk aset informasi.
- c. Mengidentifikasi kontainer dari aset informasi  
Hanya ada satu aktivitas pada langkah tiga. Perhatikan poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.
- d. Mengidentifikasi area masalah  
Aktifitas 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.
- e. Mengidentifikasi skenario ancaman  
Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini.
- f. Mengidentifikasi risiko  
Aktivitas satu pada langkah 6 menentukan *threat* skenario yang telah didokumentasikan di *Information Asset Risk Worksheet* dapat memberikan dampak bagi organisasi.
- g. Menganalisis risiko  
Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheet*. Aktivitas satu dimulai dengan melakukan 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.
- h. Memilih pendekatan pengurangan  
Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan 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



## 2. Data yang digunakan

Sumber data adalah sesuatu yang sangat penting dalam suatu penelitian yang dimaksud dengan sumber data dalam suatu penelitian adalah subjek dari mana data diperoleh sumber data yang dibagi menjadi dua macam yaitu :

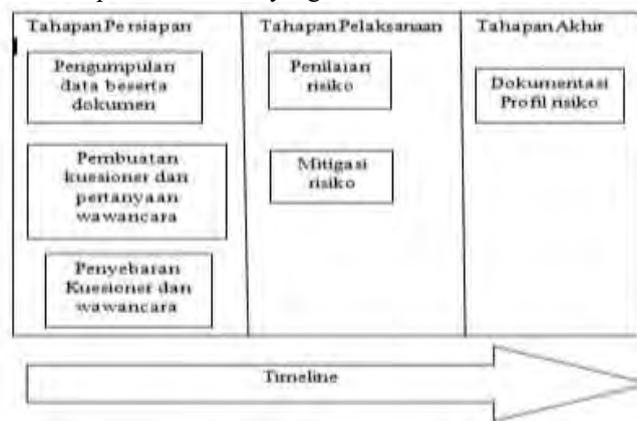
### a. Data Primer

Data primer yaitu data yang diperoleh langsung dari sumber yang diamati dan dicatat untuk pertama kalinya. Dalam hal ini data yang dihimpun adalah terkait tentang penilaian manajemen risiko untuk meminimalkan risiko terhadap implementasi teknologi informasi. Data primer ini diperoleh dengan melakukan wawancara. Penyebaran kuesioner, observasi maupun dokumentasi yang dilakukan peneliti selama berada dilapangan.

### b. Data Sekunder

Data sekunder merupakan data yang bukan diusahakan sendiri pengumpulannya oleh peneliti. Data sekunder adalah data yang mendukung atau memberi informasi yang bermanfaat berkaitan dengan penelitian ini, baik data internal maupun eksternal. Dalam hal ini data yang dihimpun adalah sejarah, visi dan misi dan profil organisasi Unjani dan Pusisfo.

Berikut adalah Gambar 2 dari penilaian risiko yang akan dilakukan:



Gambar 2 Skema Tahapan Penilaian risiko

## 3. Proses penyelesaian masalah

Tahap pertama pelaksanaan penilaian risiko dimulai menghubungi pihak-pihak pengelola divisi IT antara lain pimpinan divisi (ketua PUSISFO) sistem analisis dan *programmer* untuk mendapatkan data yang diperlukan. Tahap selanjutnya adalah melakukan wawancara guna mendapatkan informasi mengenai aset operational kritis bagi organisasi.

Langkah 1 ini terdapat dua aktivitas, diawali dengan membangun *organizational drivers* digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali *impact area* yang paling penting. Aktivitas 1 yaitu membuat definisi ukuran kualitatif yang di dokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas 2 melakukan pemberian nilai prioritas pada *impact area* menggunakan *impact area ranking worksheet* seperti pada Tabel 1.

Tabel 24 *Impact Area* – Reputasi dan Kepercayaan

<b>Impact Area</b>	<b>Low</b>	<b>Medium</b>	<b>High</b>
<b>Reputation</b>	Reputasi Sedikit Terpengaruhi; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan	Reputasi terkena dampak buruk; dan dibuthkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
<b>Customer Less</b>	Kurang dari 2% pengurangan pelanggan yang diakibatkan	2% hingga 10% pengurangan pelanggan yang diakibatkan	Lebih dari 10% pengurangan pelanggan yang diakibatkan



	hilangnya kepercayaan	hilangnya kepercayaan	hilangnya kepercayaan
--	-----------------------	-----------------------	-----------------------

Tabel 25 Skala Prioritas *Impact Area*

<i>Priority</i>	<i>Impact Area</i>
5	Reputasi dan kepercayaan
4	Finansial
3	Produktivitas
1	Keamanan dan kesehatan
2	Denda dan penalti

Langkah 2 dalam mengembangkan *Information Asset profile* dibutuhkan. Aktivitas 3 dan 4 mengumpulkan informasi mengenai informasi aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deksripsi aset informasi kritis tersebut. Aktivitas tujuh mengisi keamanan untuk *confidentiality*, *integrity* dan *availability*. Pada Tabel 3 aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

Tabel 26 *Information Asset Profilling* – Transaksi Nilai Mahasiswa

<i>Critical Asset</i>	Transaksi Nilai Mahasiswa	
<i>Rationale For Selection</i>	Informasi nilai mahasiswa ini untuk menentukan Nilai IPK mahasiswa dan untuk memberikan informasi mengenai history nilai dari setiap matakuliah	
<i>Decription</i>	Terdiri dari data nilai mahasiswa	
<i>Owner</i>	PUSISFO Akademik	
<i>Security Requirement</i>	<i>Confidentiality</i>	Informasi ini bersifat pribadi dan hanya bisa diakses oleh mahasiswa itu sendiri dan informasi ini penting bagi mahasiswa, dosen untuk cetak transkrip nilai
	<i>Integrity</i>	Informasi ini harus diisi dengan benar dan akurat sehingga hanya bisa diisi oleh dosen yang mengampu matakuliah atau bagian kemahasiswaan saja yang bisa mengubah nilai
	<i>Availability</i>	Informasi ini harus selalu tersedia bagi setiap mahasiswa
<i>Most Importan Security Requirement</i>	<p><b>Integriy Alasan:</b>            Nilai merupakan data penting bagi mahasiswa dan merupakan aset penting di bagian akademik, apabila ada kesalahan input atau data rusak itu sangat merugikan mahasiswa.</p>	

Langkah 3 Mengidentifikasi kontainer dari aset informasi



Hanya ada satu aktivitas pada langkah tiga. Perhatikan poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi seperti pada Tabel 4.

Tabel 27 *Information Asset Risk Environment* – Transaksi Nilai Mahasiswa

Data Transaksi Nilai Mahasiswa	
<i>Information Asset Risk Environment Map (Technical)</i>	
<b>Internal</b>	
<i>Container Description</i>	<i>Owner (s)</i>
<b>Modul:</b> SIM Akademik	Dosen, Bagian Kemahasiswaan Jurusan
Input transaksi Nilai Mahasiswa dan disimpan dalam database Mahasiswa	
<b>External</b>	
<i>Container Description</i>	<i>Owner (s)</i>
<b>Aplikasi:</b> Web Nilai	Mahasiswa
Mahasiswa dapat melihat Nilai	

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 seperti pada Tabel 5.

Tabel 28 *Area Of Concern*

No	<i>Area Of Concern</i>
1.	Pengolahan data mahasiswa yang banyak akan menyebabkan kesalahan <i>input</i> data oleh bagian fakultas administrasi atau pihak dosen
2.	Penyebaran hak akses ( <i>password</i> ) terhadap sistem informasi mahasiswa yang dapat diakses oleh bagian pussisfo Unjani
3.	keamanan dalam sistem sehingga sistem bisa di <i>hacker</i> /di eskploitasi oleh pihak luar
4.	<i>Bug/error</i> yang terdapat pada sistem informasi mahasiswa
5.	Kesalahan yang disebabkan oleh kejadian yang tak terduga (tersambar petir, listrik konslet, atau kebakaran) sehingga <i>server</i> rusak
6.	Penggunaan sistem informasi oleh <i>staff</i> yang tidak berwenang dalam akses transaksi nilai mahasiswa
7.	Data nilai mahasiswa di ubah oleh pihak yang tidak berwenang

Langkah 5 Mengidentifikasi skenario ancaman

Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas seperti pada Tabel 6.

Tabel 29 *Properties Of Threat* - Transaksi Nilai Mahasiswa

No	<i>Area Of Concern</i>	<i>Threat Of Properties</i>	
1	Pengolahan data mahasiswa yang banyak akan menyebabkan kesalahan input data oleh bagian fakultas administrasi atau pihak dosen	<b>1. Actors</b>	Staff Jurusan
		<b>2. Means</b>	SIM Akademik
		<b>3. Motives</b>	Human eror
		<b>4. Outcome</b>	<i>Modification</i> <i>Interruption</i>
		<b>5. Security Requirement</b>	penambahan validasi data input nilai pada setiap field-field

Langkah 6 Mengidentifikasi risiko



Aktivitas satu pada langkah 6 menentukan *threat* skenario yang telah didokumentasikan di *Information Asset Risk Worksheet* dapat memberikan dampak bagi organisasi seperti pada Tabel 7.

Tabel 7 Perhitungan *Relative Score*

<i>Impact Area</i>	<i>Priority</i>	<i>Low</i>	<i>Medium</i>	<i>High</i>
Reputasi dan kepercayaan	5	5	4	9
Finansial	4	8	7	15
Produktivitas	3	5	1	6
Keamanan dan kesehatan	2	2	4	6
Denda dan penalti	1	7	3	10

Langkah 7 Menganalisis risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheet*. Aktivitas satu dimulai dengan melakukan 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 seperti pada Tabel 8.

Tabel 8 Analisis Risiko – Transaksi Nilai Mahasiswa

No	<i>Area Of Concern</i>	<i>Risk</i>			
1.	Pengolahan data mahasiswa yang banyak akan menyebabkan kesalahan input data oleh bagian fakultas administrasi atau pihak dosen	<i>Consequences</i>	Membutuhkan waktu untuk memperbaiki nilai yang salah input data		
		<i>Severity</i>	<i>Impact Area</i>	<i>Value</i>	<i>Score</i>
			Reputasi dan Kepercayaan	Med	4
			Finansial	Low	8
			Produktivitas	High	6
			Keamanan dan kesehatan	Low	2
			Denda dan Penalti	Low	7
<i>Relative Score</i>			27		

Langkah 8 - Memilih pendekatan pengurangan

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua seperti pada Tabel 9, Tabel 10, Tabel 11 melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

Tabel 9 *Relative Risk Matrix*

<i>Risk Score</i>		
30 To 45	16 To 29	0 To 15
POOL 1	POOL 2	POOL 3

Tabel 10 *Mitigation Approach*

<i>Pool</i>	<i>Mitigation Approach</i>
Pool 1	Mitigate
Pool 2	Mitigate Or Defer
Pool 3	Accept

Tabel 11 *Mitigation* Risiko berdasarkan *Area Of Concern*

<i>Risk Mitigation</i>
------------------------



<b>Area Of Concern</b>	Pengolahan data mahasiswa yang banyak akan menyebabkan kesalahan input data oleh bagian fakultas administrasi atau pihak dosen
<b>Action</b>	<b>Mitigate Or Defer</b>

## KESIMPULAN

Universitas Jenderal Achmad Yani (UNJANI) adalah sebuah perguruan tinggi dibawah naungan Yayasan Kartika Eka Paksi yang terletak di Bandung dan Cimahi. Universitas Jenderal Achmad Yani ini memiliki 7 Fakultas dan memiliki 23 jurusan. Sebagai sebuah lembaga pendidikan tentunya mempunyai sistem informasi untuk membantu tercapainya rencana strategi lembaga tersebut. Untuk menjalankan sistem informasi UNJANI tentunya memiliki teknologi informasi. Dalam penggunaan teknologi informasi tersebut tidak lepas dari risiko yang mungkin akan timbul dan dapat mengancam *asset* yang dimiliki baik material maupun *non-material*, seperti waktu 6 tahun yang lalu yaitu kegagalan sistem yang tidak berfungsinya data *Center* Unjani karena aliran listrik utama dari PLN terputus. Untuk meminimalisir risiko tersebut dikelola dan dicari langkah pencegahan yang tepat dengan menggunakan kerangka kerja tertentu.

*Octave Allegro* merupakan salah satu metode manajemen risiko sistem informasi yang dapat diterapkan di perguruan tinggi tanpa memerlukan keterlibatan yang ekstensif di dalam organisasi dan difokuskan kepada aset informasi yang kritis untuk keberlangsungan organisasi. Dan dari hasil penilaian risiko dapat terlihat ancaman terhadap aset informasi yang dimiliki oleh perusahaan atau organisasi itu.

## DAFTAR PUSTAKA

- Deni Ahmad Zakaria, R. t. D., H., 2013. "Manajemen risiko sistem informasi akademik pada perguruan tinggi menggunakan metode octave allegro". *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, pp. 1-7.
- Henki Bayu Seta, T., T. R., 2017. "Manajemen Risiko Aplikasi Pembelajaran Berbasis Online Pada Universitas Dengan Menggunakan Metode Octave Allegro", Volume ISSN : 2302- 3805, pp. 1-6.
- Joshua Jenriwan L Tobing, A. K. P., 2015. "Analisis Manajemen Resiko untuk Evaluasi Asset menggunakan Metode Octave Allegro". *Expert- Jurnal Manajemen Sistem Informasi Dan Teknologi*, Volume 05, Nomor 01, Juni 2015, pp. 1-7.
- Maliki, I., 2010. "Manajemen risiko teknologi informasi untuk keberlangsungan layanan publik menggunakan framework information technology infrasturcture library (itil versi 3)". *Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010)*, pp. 1-6.
- Nugraha, U., 2016. "Manajemen risiko sistem informasi pada perguruan tinggi menggunakan kerangka kerja nist sp 800-300", Volume ISSN : 2503-2844, pp. 1-6.
- Richard A. Caralli, J. F. L. R. W. R., May 2007. *Introduction OCTAVE Allegro : Improving the information Security Risk Assesment Process*. s.l.:Carnegie Mellon.
- Supradono, B., 2009. "Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, And Vulnerability Evaluation)", "Volume Vol.2 No 1, pp. 1-5.
- Rizal, I. C. (n.d.). *Analisis sistem informasi akademik onlie di universitas diponegoro semarang*, 1-8.
- Rosini, M. R. (n.d.). *Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allgero*, 1-9.
- Sucahyo, D. F. (n.d.). *Jurnal Sistem Informasi MTI-UI*, Volume 4, Nomor 1, ISBN 1412-8896. Audit sistem informasi/teknologi informasi dengan kerangka kerja cobit untuk evaluasi manajemen teknologi di universitas xyz, 1-10.
- Dr.Mamduh M.Hanafy, M. *Modul Risiko, Proses Manajemen Risiko dan Enterprise Risk Manajemen*.
- Eki Pujastuti, A. N. (2016). *Seminar Nasional Teknologi Informasi dan Multimedia (STMIK AMIKOM YOGYAKARTA)*. "Analisis manajemen risiko pada penggunaan sistem informasi "smart pmb" di stmik amikom Yogyakarta, 1-6.



