

**ANALISIS MANAGEMEN RESIKO TEKNOLOGI INFORMASI PADA WEBSITE**

**Dwi Yana Ayu Andini<sup>1</sup>, Aviv Fitria Yulia<sup>2</sup>**

<sup>1</sup>Program Studi Rekayasa Perangkat Lunak, Fakultas Teknologi dan Informatika  
 Universitas Aisyah Pringsewu

<sup>2</sup>Program Studi Rekayasa Perangkat Lunak, Fakultas Teknologi dan Informatika  
 Universitas Aisyah Pringsewu

[dwiyana@aisyahuniversity.ac.id](mailto:dwiyana@aisyahuniversity.ac.id), [avivfitriayulia0@gmail.com](mailto:avivfitriayulia0@gmail.com)

<b>Article Info</b>	<b>ABSTRAK</b>
<p><b>Kata Kunci:</b></p> <p>Teknologi Infomasi                  Website                  Sistem Informasi                  ISO 31000                  OCTAVE</p>	<p>Pada saat ini teknologi informasi memberikan pen- garuh besar terhadap kehidupan kita, informasi digital yang saat ini berkembang adalah sistem informasi berbasis website yang telah digunakan diberbagai organisasi atau intitusi untuk mem- berikan informasi yang tepat dan bermanfaat. Peran teknologi informasi khususnya website pada suatu perusahaan ataupun instansi hal yang penting dan tidak dapat dipisahkan dari proses bisnis ataupun kegiatan dalam kelembagaan tersebut. Akan tetapi, tidak dapat dihindari penggunaan dari implementasi terse- but dapat menimbulkan risiko yang tidak diinginkan mengancam dari proses bisnis itu sendiri. Hal ini harus menjadi perhatian khusus demi keamanan informasi. Untuk menghindari risiko- risiko itu terjadi maka perlunya upaya pengukuran terhadap risiko teknologi informasi pada website.</p>
<p><b>Keywords:</b></p> <p>COBIT 5                  Data Mining                  Naïve Bayes                  Frame Work                  Web Qual</p>	<p><b>ABSTRACT</b></p> <p>At present, information technology has a significant influence on our lives. The evolving digital information is in the form of website-based information systems, which are widely utilized by various organizations or institutions to provide accurate and useful information. The role of information technology, especially websites, in a company or institution is crucial and inseparable from the business processes or activities within that institution. However, the unavoidable use of such implementations can pose unwanted risks that threaten the business processes themselves. This should be a special concern for the security of information. To prevent such risks, efforts to measure information technology risks on websites are necessary.</p>
	<p style="text-align: right;"><i>This is an open access article under the <a href="https://creativecommons.org/licenses/by-sa/4.0/">CC BY-SA</a> license.</i></p> 

**Penulis Korespondensi:**

Dwi Yana Ayu Andini,  
 Program Studi Rekayasa Perangkat Lunak  
 Universitas Aisyah Pringsewu, Indonesia  
 Email: [dwiyana@aisyahuniversity.ac.id](mailto:dwiyana@aisyahuniversity.ac.id)

**1 PENDAHULUAN**

Tidak dapat dipungkiri bahwa perkembangan dunia internet saat ini mencapai suatu tahapan begitu cepat, sehingga kita dapat menemukan dengan cepat berbagai jasa pelayan inter- net. internet hingga saat ini menjadi kebutuhan manusiatelah melalui perjalanan yang cukup panjang. pada awalnya internet adalah jaringan informasi (pada akhir 1960-an, mulai tahun 1969) yang di kembangkan oleh Dapertemen Pertahanan dan Keamanan Amerika serikat (DoD = Departement of De- fense) USA dengan tujuan berjaga-jaga (penagulangan) jika terjadi gangguan pada jarinagn komunikasi umum,khususnya pengaruhnya pada sistem komunikasi militer mereka sebagai proyek yang strategis [1]. Peran teknologi khususnya dalam teknologi informasi begitu cepat yang sangat berpengaruh besar pada aspek kehidupan salah satunya adalah oraganisasi maupun instansi akan men- gelola sistem informasi berbasis websiteyang menghasilkan suatu informasi yang tepat dan bermanfaat. Peran teknologi informasi khususnya website pada suatu perusahaan ataupun instansi hal yang penting dan tidak dapat dipisahkan dari proses bisnis ataupun kegiatan dalam kelembagaan tersebut. Akan tetapi, tidak dapat dihindari penggunaan dari implemen- tasi tersebut dapat menimbulkan risiko yang tidak diinginkan mengancam dari proses bisnis itu sendiri.Hal ini harus menjadi perhatian khusus demi keamanan informasi. Untuk menghin- dari risiko-risiko itu terjadi maka perlunya upaya pengukuran terhadap risiko teknologi informasi pada website. [2]. Ancaman dan risiko muncul dalam sistem yang mengganggu bahkan dapat melumpuhkan aktivitas yang menyebabkan sistem tidak berjalan secara optimal.agar organisasi atau instansi dapat menghindari kemungkinan ancaman risiko itu

muncul maka diperlukan analisis risiko terhadap sistem, jika hal tersebut terjadi maka dapat langsung diberikan penanganan serta perbaikan dari ancaman risiko tersebut [3]. Management risiko yang dinyatakan oleh Noval [3] pada ISO 31000 adalah efek dari ketidakpastian pada tujuan yang positif maupun negatif. Dengan diringin penerapan sumber daya tidak terkoordinasi dan ekonomis untuk meminimalkan, memantau, dan mengontrol kemungkinan dampak dari peristiwa yang tidak menguntungkan atau memaksimalkan realisasi peluang. Dalam teknologi informasi didalam Website terdapat beberapa risiko terkait dengan keamanan informasi. Karena terdapat sebuah data-data yang bersifat privasi sehingga harus dilindungi dengan sebuah sistem keamanan. Dengan adanya sistem keamanan maka akan meminimalisir tingkat pengambilan data secara ilegal walaupun tidak sepenuhnya aman namun beberapa celah risiko yang akan diperhitungkan. Untuk menghindari risiko-risiko itu terjadi maka perlunya upaya pengukuran terhadap risiko teknologi informasi pada web seperti ISO 31000 dan pendekatan OCTAVE.

## 2 METODE PENELITIAN

Metode penelitian manajemen risiko pada sistem informasi website digunakan untuk menganalisa pada bagian bagian atau struktur yang memungkinkan terjadinya sebuah permasalahan yang berdampak terhadap sebuah instansi yang menaunginya. Berikut adalah beberapa metode – metode yang digunakan :

### 2.1 ISO 31000

Metode ISO 31000 bertujuan melakukan pencegahan, penanganan dan pemeliharaan terhadap sistem dan aset pendukung kinerja sistem di masa depan dengan melakukan identifikasi risiko, pemeliharaan risiko dan penilaian risiko. Penelitian ini akan menghasilkan risiko aset sistem swiftnya yang membutuhkan koneksi jaringan dan asupan listrik yang konstan agar perangkat dapat berjalan untuk mendukung jalannya sistem secara optimal [4].

Metode ISO 31000 ini dapat digunakan berbagai kelompok, perusahaan swasta, perusahaan publik, nirlaba, ataupun perseorangan. ISO 31000 memiliki standar yang dapat digunakan selama masa hidup suatu organisasi untuk berbagai kegiatan, proses, fungsi, proyek, produk, jasa, aset, operasi dan pengambilan keputusan [5]. Ada lima kegiatan risiko yang masuk kedalam proses manajemen risiko yaitu :

- komunikasi dan konsultasi, menentukan konteks
- assesment risiko
- perlakuan risiko dan monitoring serta review
- Identifikasi risiko
- analisis risiko dan evaluasi risiko

ISO 31000: 2009 mengartikan bahwa asesmen risiko adalah keseluruhan proses analisis risiko, identifikasi risiko, dan evaluasi risiko.

- a. Identifikasi Risiko (Risk Identification) identifikasi akan dilakukan wawancara langsung pada pihak yang bertanggung jawab yang mencakup penilaian berdasarkan pencatan dan pengalaman, proses tersebut adalah :
  - Identifikasi teknologi informasi yang dimiliki oleh organisasi
  - Identifikasi ancaman pada setiap teknologi informasi
  - Identifikasi kemungkinan risiko yang diakibatkan oleh adanya ancaman
  - Identifikasi dampak yang akan diterima oleh organisasi tersebut
- b. Analisis Risiko (Risk Analysis) adalah penerapan secara kualitatif. Kualitatif itu sendiri relatif cepat dan mudah untuk mengidentifikasi dampak (impact) dan jangka panjang bahan evaluasi untuk pemeringkatan risiko. Analisa secara kualitatif menjadi proses penentuan prioritas suatu analisis atau tindakan respon yang lebih jauh dengan mengukur dan mengkombinasikan probabilitas terjadinya risiko serta dampak dari risiko tersebut. Analisa ini menjadi tahapan yang paling efektif dan dapat menghemat biaya, risiko yang memiliki tingkat prioritas tinggi (high-priority risk) dapat melakukan improvisasi terhadap performansi proyek yang menjadi fokus organisasi atau perusahaan, jika diperlukan analisa kualitatif ini dapat digunakan sebagai dasar prioritas risiko. Setelah peluang atau probabilitas (likelihood) serta dampak selesai diidentifikasi, selanjutnya lakukan evaluasi guna mengetahui risiko prioritas yang ditangani dahulu.
- c. Evaluasi Risiko (Risk Evaluation) adalah tahapan menbandingkan risiko terkait diatas dengan ketentuan yang telah distandarkan oleh risiko tersebut, jika low yang diartikan rendah atau dapat diterima, moderate yang diartikan sebagai sedang atau yang perlu diwaspadai, setelah itu adalah high yang diartikan sebagai tinggi atau tidak dapat diterima, dan diprioritaskan untuk mitigasi atau penanganannya.

## 2.2 OCTAVE (Operationally Critical Threat, Assets and Vulnerability Evaluation)

Metode OCTAVE (Operationally Critical Threat, Assets and Vulnerability Evaluation) adalah metode yang dikembangkan oleh universitas Carnegie Mellon, manajemen ini digunakan untuk melakukan manajemen risiko yang menggabungkan analisis perilaku organisasi, dan kelemahan teknologi [6]. Tujuan menggunakan metode Octave ini adalah untuk dapat mengetahui dan mengelola faktor risiko terhadap keamanan sistem informasi serta memberikan rekomendasi dari data hasil temuan faktor risiko keamanan didalam Website [7]. Manfaat dari penelitian ini adalah memberikan gambaran risiko celah keamanan dari sistem informasi layanan publik pada Website, sehingga dapat meningkatkan keamanan pada sistem informasi layanan publik yang digunakan. Ada tiga jenis metode oktave yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro [8]. seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamanan sistem informasi berbasis risiko disebut OCTAVE. sedangkan metode yang disederhanakan yang fokus pada aset informasi disebut OCTAVE Allegro. metoda workshop-style dan kolaboratif dapat di lakukan pada OCTAVE Allegro. OCTAVE Allegro terdiri dari delapan langkah dibagi dalam empat fase.

<b>LIKELIHOOD</b>	<i>Certain / Pasti Terjadi</i> (5)	Moderate	Moderate	High	High	High
	<i>Likely / Sering</i> (4)	Low	Moderate	High	High	High
	<i>Possible / Kadang</i> (3)	Low	Low	Moderate	High	High
	<i>Unlikely / Jarang</i> (2)	Low	Low	Moderate	Moderate	High
	<i>Rare / Sangat Jarang</i> (1)	Low	Low	Low	Moderate	Moderate
		<i>Insignificant / Sangat Kecil</i> (1)	<i>Minor / Kecil</i> (2)	<i>Moderate / Biasa</i> (3)	<i>Major / Besar</i> (4)	<i>Catastrophic / Sangat Besar</i> (5)
		<b>IMPACT</b>				

Gambar 2.1 Metode Octave Allegro

Ket :

	H : High Risiko (Risiko Tinggi)
	M : Moderate Risk (Risiko Sedang)
	L : Low Risk (Risiko Rendah)

Pada proses pengerjaan metode OCTAVE Allegro dimana pada metode ini evaluasi dilakukan secara rinci terhadap risiko kemudian memberikan penilaian risiko. Yang pertama dilakukan adalah proses analisis, ke dalam 4 fase utama dan 8 tahap sesuai dengan metode OCTAVE Allegro.

- a. Fase pertama yaitu Establish Driver, pada fase pertama dimulai dengan menetapkan kriteria pengukuran risiko pada lingkup Website.
- b. Fase kedua Profile Assets membuat profile yang dimiliki oleh Website.
- c. Fase ketiga yaitu Identify Threat, mengidentifikasi ancaman terhadap aset informasi Pada Website.
- d. Fase terakhir Identify and Mitigate Risk, risiko terhadap aset diidentifikasi dan dilakukan mitigasi.

Level Risiko	Keterangan
High Risk	Risiko yang berbahaya yang harus diatasi secepatnya. Risiko
Moderate Risk - Risiko Sedang	Risiko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan. Risiko
Low Risk - Risiko Rendah	Risiko ini dapat diabaikan dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh paling kecil.

Gambar 2.2 Level Risiko



Gambar 2.3 Metode Octave Allegro

Pada gambar diatas adalah fase fase pada metode OCTAVE Allegro. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) mendefinisikan komponen- komponen penting secara komprehensif, sistematis, berbasis konteks (context-driven) evaluasi risiko keamanan informasi. Dengan menggunakan metode OCTAVE, organisasi dapat membuat perlindungan terhadap informasi berbasis pengam- bilan keputusan risiko berdasarkan CIA (Confidentiality, In- tegrity, Authentication) untuk aset teknologi informasi kritis [9]. Metode OCTAVE Allegro pada Gambar 1 terdapat 8 tahapan didalam 4 fase utama. Menurut [8] Berikut adalah penjelasan dari 8 tahap sesuai dengan Metode OCTAVE Alle- gro.

- Langkah pertama yaitu membangun Kriteria Penguku- ran Risiko yang terdapat dua aktivitas, yang diawali dengan membangun organizational drivers dapat digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, yang terpenting dapat mengenali impact area. Risk measurement criteria adalah aktivitas pertama yang dilakukan untuk mem- buat definisi ukuran kualitatif yang didokumentasikan. Setelah itu Impact Worksheet adalah aktivitas kedua untuk melakukan pemberian nilai prioritas impact area.
- Langkah kedua yaitu mengembangkan Profil Aset Infor- masi yang terdiri dari delapan aktivitas, yang pertama identi- fikasi aset informasi, yang kedua lakukan penilaian risiko ter- struktur pada aset yang kritis. langkah ketiga mengumpulkan informasi mengenai information aset yang penting, langkah keempat dengan membuat dokumentasi alasan pemilihan aset informasi kritis. langkah kelima membuat deskripsi aset in- formasi kritislangkah enam mengidentifikasi kepemilikan dari aset informasi kritis. langkah ketujuh mengisi kebutuhan kea- manan untuk confidentiality, integrity dan availaibility. Langkah kedelapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.
- Langkah ketiga yaitu mengidentifikasi Kontainer dari Aset Informasi Hanya ada satu aktivitas pada langkah tiga, yang menjadi point perhatian adalah cara aset informasi dilin- dungi mulai dengan keaman dan dan konsep dari kontainer aset informasi, tingkat perlindungan atau pengamanan aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.
- Langkah keempat adalah Mengidentifikasi Area Masalah Aktivitas langkah ini diawali mulainya bertukr pikiran dengan mencari ancaman yang mungkin mengancam aset informasi dengan pengembangan profil risiko itu sendiri. Dengan dipan- dnya dokumen Information Asset Risk Environment Maps dan Information Asset Risk Worksheet disimpulkan area of concern. Dokumen Information Asset Risk Worksheet mem- berikan pedoman dengan lakukan review dari kontainer untuk membuat Area of Concern dan mendokumentasikan setiap Area of Concern.
- Langkah lima yaitu Mengidentifikasi Skenario Ancaman, pada langkah lima yaitu dalam melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan Ap- pendix C – Threat Scenarios Questionnaires. Untuk skenario yang umum dapat dilakukan melengkapi Information Asset Risk Worksheets .
- Langkah enam yaitu Mengidentifikasi Risiko hal ini da- pat memberikan dampak bagi organisasi dengan menentukan threat scenario yang telah didokumentasikan di Information Asset Risk Worksheet.
- Langkah tujuh yaitu Menganalisis Risiko hal ini mengacu pada dokumentasi terdapat pada Information Asset Risk Work- sheet yang harus dilakukan. hal pertama dilakukan mereview risk measurement criteria setelah itu menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko
- Langkah delapan yaitu Memilih Pendekatan Penguran- gan, menyusun setiap risiko yang diidentifikasi berdasarkan nilai risikonya.ketika hal ini dilakukan akan mempermudah untuk melakukan pengambilan keputusan mitigasi. selanjutnya melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

### 3 HASIL DAN ANALISIS

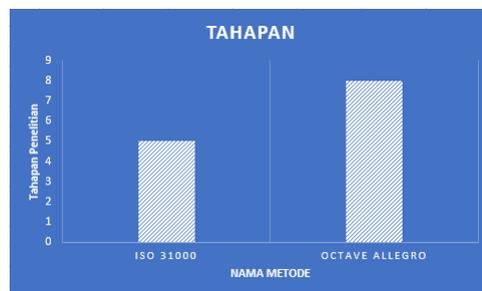
Pada kedua metode yaitu ISO 31000 dan OCTAVE Allegro terdapat beberapa spesifikasi dan kriteria pada masing-masing metode. Pada metode ISO 31000 metode bersifat kualitatif dan kuantitatif. Metode ISO 31000 yang bersifat kualitatif yaitu berorientasi pada hal-hal yang umumnya tidak dapat dihitung atau didefinisikan dengan angka. Sedangkan yang bersifat kuantitatif data tidak dapat didefinisikan dengan angka sehingga data tidak dapat dihitung [10]. Dan yang selanjutnya adalah metode OCTAVE Allegro sama dengan metode ISO 31000 dimana data bersifat kualitatif dapat dihitung dan kuantitatif dengan data yang tidak dapat dihitung juga.

Berikut ini adalah graph dari 3 buah metode NIST, OCTAVE dan ISO 31000 berdasarkan tahapan yang dilakukan pada proses pengolahan data seperti pada gambar 4.

**Tabel 4 Perbandingan Metode Manajemen Risiko Sistem Informasi Akademik**

No	Metode	Ref	Tipe	Proses
1	ISO 31000	[9] [2] [4] [10]	Kualitatif	<ul style="list-style-type: none"> <li>• komunikasi dan komunikasi</li> <li>• menentukan kontak</li> <li>• assessment risiko</li> <li>• perlakuan risiko dan monitoring serta review.</li> <li>• Identifikasi risiko</li> <li>• analisis risiko dan evaluasi risiko</li> </ul>
2	Octave Allegro	[6] [7] [8]	Kualitatif	<ul style="list-style-type: none"> <li>• Establish Driver</li> <li>• Membangun Kriteria Pengukuran Risiko</li> <li>• Profile Assets</li> <li>• Mengembangkan Profil Aset Informasi</li> <li>• Mengidentifikasi Kontainer dari Aset Informasi</li> <li>• Identify Threat</li> <li>• Mengidentifikasi Area Masalah</li> <li>• Mengidentifikasi Skenario Ancaman</li> <li>• Identify and Mitigate Risk</li> <li>• Mengidentifikasi Risiko</li> <li>• Menganalisis Risiko</li> <li>• Meneliti Pendekatan</li> </ul>

Dari tabel diatas dapat kita lihat perbandingan tahapan dimana metode OCTAVE Allegro lebih rinci daripada metode yang ISO 31000. Berikut adalah grafik dari kedua metode setelah dilakukan analisa pada metode-metode tersebut.

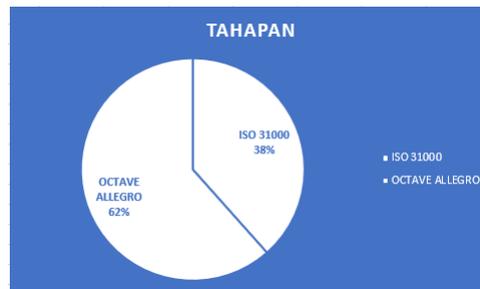


Gambar 3.1 Graph Tahapan Metode

Berdasarkan hasil analisa terhadap 2 metode yang telah dilakukan analisa dapat disimpulkan bahwa metode manajemen risiko informasi WEB menggunakan OCTAVE Allegro memiliki tahapan yang relatif lebih terperinci dan evaluasi yang lebih kompleks karena banyak tahapan yang digunakan. Metode OCTAVE Allegro memiliki 8 tahapan untuk membangun kriteria pengukuran risiko dimana pada tahapan tersebut terdapat 4 fase yang setiap fasenya terdapat 8 tahapan yang terbagi dalam 4 fase. Dalam hal pemetaan metode OCTAVE Allegro sangat detail dan teliti dibanding tahap metode yang lain. Keran pada metode ISO 31000 hanya terdapat 5 tahap pengolahan data. Selain itu hasil output pada Metode OCTAVE Allegro lebih detail dimana pada setiap tahapan terdapat setiap sub-sub hasil pengolahan data. Penilaian risiko menggunakan OCTAVE Allegro adalah membangun kriteria pengukuran risiko. Terdapat 2 aktivitas utama yakni menentukan kriteria pengukuran risiko pada tiap

impact area, dan menentukan prioritas impact area. Dalam menentukan kriteria pengukuran risiko untuk impact area reputasi dan kepercayaan nasabah. Kriteria pertama adalah reputasi yang mengacu kepada dampak risiko terhadap reputasi perusahaan. Dampak terhadap reputasi dikatakan low jika reputasi sedikit / tidak terlalu terpengaruh, dan hanya sedikit atau bahkan tidak memerlukan usaha untuk memperbaiki reputasi. Dikatakan moderate bila dampak berpengaruh terhadap reputasi dan memerlukan usaha untuk memperbaiki. Dikatakan high bila dampak merusak reputasi dan reputasi tidak dapat diperbaiki [7]

Dalam hasil analisa kuntari dkk [7] setiap perusahaan atau organisasi akan terlihat ancaman terhadap aset informasi yang mungkin akan timbul dan dapat mengancam aset yang dimiliki baik material maupun non material. Sedangkan dalam penelitian [8] tentang hasil manajemen risiko OCTAVE Allegro salah satu 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. Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada aset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi. Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah – langkah pemulihan jika skenario ancaman benar – benar terjadi.



Gambar 3.2 Grafik Persentase Metode

#### 4. KESIMPULAN

- Berdasarkan analisa yang telah dilakukan pada 2 metode dari jurnal dengan melakukan review dapat disimpulkan bahwa:
- Dari 2 metode yang digunakan (OCTAVE Allegro, ISO 31000) yang paling sesuai digunakan adalah OCTAVE Allegro. Karena memiliki tahapan yang lebih rinci dibandingkan dengan Metode ISO 31000 yang menggunakan 5 tahap, sedangkan metode OCTAVE Allegro 8 tahap yang terdapat pada persentase metode dalam Gambar 3.
  - Setiap metode memberikan perancangan tentang manajemen risiko dan juga pencegahan terhadap ancaman kedepannya.

#### DAFTAR PUSTAKA

- [1] A. Elanda and D. Tjahjadi, “Analisis Manajemen Risiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute of Standards and Technology) Sp 800-30 (Studi Kasus Disinfolahaatau Mabes Tni Au),” *Infoman’s*, vol. 12, no. 1, pp. 1–13, 2018.
- [2] M. Miftakhatun, “Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000,” *Journal of Computer Science and Engineering (JCSE)*, vol. 1, no. 2, pp. 128–146, 2020.
- [3] A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko, “Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University),” *e-Proceeding of Engineerin*, vol. 2, no. 2, pp. 6201–6208, 2015.
- [4] A. Rahmawati and A. F. Wijaya, “Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP,” *Jurnal SITECH : Sistem Informasi dan Teknologi*, vol. 2, no. 1, pp. 13–20, 2019.
- [5] A. Muslimin, A. S. Raharjo, and S. Lestari, “Manajemen Risiko Teknologi Informasi Terkait Pandemi COVID-19 Pada SDN 1 Negara Batin Menggunakan Framework COBIT 5 dan ISO / IEC 31000,” pp. 88–94, 2020.
- [6] R. Noviana, “IMPLEMENTASI METODE OCTAVE PADA PENGELOLAAN MANAJEMEN RESIKO,” 2021.
- [7] N. L. Kuntari, Y. H. Chrisnanto, and ..., “Manajemen Risiko Sistem Informasi di Universitas Jenderal Achmad Yani Menggunakan Metoda Octave Allegro,” *Seminar Nasional . . .*, 2018. [Online]. Available: <http://prosiding.uika-bogor.ac.id/index.php/semnati/article/view/106>
- [8] D. A. Jakaria, R. T. Dirgahayu, and Hendrik, “Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro,” *Fakultas Hukum UII*, pp. 37–42, 2013.
- [9] S. K. PANDEY, “A Comparative Study of Risk Assessment Methodologies for Information Systems,” *Bulletin of Electrical Engineering and Informatics*, vol. 1, no. 2, pp. 111–122, 2012.
- [10] K. G. F, “Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000,” *Angewandte Chemie International Edition*, 6(11), 951–952., 2016.