Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI) 2023
Surabaya, 6 – 7 September 2023

ANALISIS KEAMANAN WEBSITE DINAS PERHUBUNGAN PROVINSI JAWA TIMUR MENGGUNAKAN METODE OCTAVE ALLEGRO DAN FMEA

SECURITY ANALYSIS OF THE EAST JAVA PROVINCIAL TRANSPORTATION AGENCY WEBSITE USING THE OCTAVE ALLEGRO METHOD AND FMEA

Heldha Ayu Setia[1*], Eristya Maya Safitri[1], Verina Renata Putri[1], Cintami Prasista Wibowo[1]
*E-mail: heldadewa15012003@gmail.com

[1]Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur

Abstrak

Adaptasi teknologi memerlukan penyesuaian yang harus selalu berkembang. Kemajuan teknologi juga akan terus berlanjut, sehingga setiap organisasi maupun instansi pemerintah pun harus mengikuti perkembangan tersebut agar tetap relevan dan kompetitif. Salah satu penerapannya pada instansi pemerintah yaitu Dinas Perhubungan Provinsi Jawa Timur. Dalam memastikan kualitas penyampaian manfaat dan informasi yang baik kepada masyarakat, dibentuknya *website* resmi https://dishub.jatimprov.go.id/ pada laman mereka. Akan tetapi, tentunya hal itu tidak akan terlepas dari serangan *cyber* yang ingin untuk menyusup ke dalam website untuk merusak atau mengubah konten di dalamnya. Maka dari itu, artikel ini menggunakan metode pendekatan OCTAVE untuk menganalisis secara menyeluruh terkait aset informasi pada website, mengidentifikasi ancaman potensial, lalu mengevaluasi kerentanan dan kelemahan dalam perlindungan keamanan website yang ada. Untuk mengevaluasi sistem keamanan yang ada pada website, FMEA digunakan untuk mengevaluasi dan menilai dampak risiko dari aset informasi yang ada dan menentukan nilai RPN (Risk Priority Number) dari aset kritis. Hasil menunjukan bahwa risiko keamanan pada website memperoleh 4 tingkatan level pada pengukuran nilai risiko yaitu tinggi, rendah, sedang, sangat rendah sehingga sangat jarang terjadi risiko kerawanan dan ancaman, meskipun jarang dilakukan pengecekan bila tidak terjadi hal-hal yang mencurigakan.
Kata kunci: *keamanan, website, octave, fmea, risiko*

Abstract

Technological adaptation requires continuous development and adjustment. Technological advancements will continue to progress, prompting organizations and government institutions to keep up with these advancements to remain relevant and competitive. One such implementation is seen in the government institution of the East Java Provincial Transportation Office. To ensure the quality delivery of benefits and information to the public, they have established an official website at https://dishub.jatimprov.go.id/. However, this is not without the risk of cyber attacks aiming to infiltrate the website and disrupt or manipulate its content. Therefore, this article utilizes the OCTAVE approach to comprehensively analyze the information assets of the website, identify potential threats, and evaluate vulnerabilities and weaknesses in the existing website security measures. To evaluate the existing security system of the website, FMEA is used to assess and determine the risk impact of the information assets and calculate the Risk Priority Number (RPN) for critical assets. The results indicate that the security risks on the website are classified into four levels: high, low, moderate, and very low. Consequently, the occurrence of vulnerability and threats is very rare, although regular checks are infrequently conducted unless suspicious activities arise.
***Keywords**: security, website, octave, fmea, risk.*

1. PENDAHULUAN

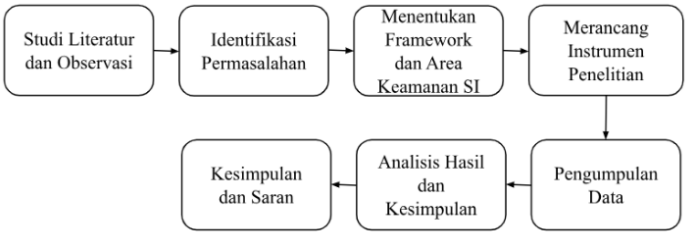
Dalam memaknai pentingnya penerapan teknologi demi menunjang keberlangsungan suatu instansi merupakan suatu hal yang krusial dan strategis [1]. Penerapan teknologi informasi dalam instansi pemerintah, termasuk Dinas Perhubungan Provinsi Jawa Timur, memiliki peran penting dan strategis dalam meningkatkan kinerja dan memberikan layanan yang efisien. Dengan menyediakan aksesibilitas informasi melalui *website* resmi mereka pada laman https://dishub.jatimprov.go.id/, Dinas Perhubungan Provinsi Jawa Timur menyediakan informasi yang aktual, relevan, dan efektif, seperti Profil Dinas, Video Kegiatan, Informasi Pelayanan, Program Mudik Gratis, dan laporan penting lainnya.

Gangguan yang diakibatkan oleh tindakan *cybercrime* terutama pada layanan informasi digital yang merupakan *website* resmi dari Dinas Perhubungan Provinsi Jawa Timur ini dapat berupa serangan *defacement*, DDos, pencurian data, serangan *hacker* dalam rangka mengambil alih fungsi admin, dan banyak lainnya. Oleh karena itu, artikel ini bertujuan untuk menganalisis tingkat risiko keamanan pada *website* resmi Dinas Perhubungan Provinsi Jawa Timur serta menginvestigasi dampak merugikan dan gangguan yang ditimbulkan oleh tindakan *cybercrime* dengan mengidentifikasi cara-cara mitigasi yang efektif guna menjaga keberlangsungan instansi. Studi literatur pada penelitian sebelumnya membahas tentang manajemen risiko aset TI yang mengukur praktik keamanan menggunakan OCTAVE dan FMEA, hasil yang diperoleh pada artikel ini mengidentifikasi 19 risiko dan 22 kejadian ancaman terkait aset kritis, beberapa risiko memiliki lebih dari satu ancaman, sehingga direkomendasikan pengembangan praktik keamanan, selain itu diidentifikasi kontrol dan klausul dalam standar ISO untuk mitigasi risiko dan implementasi [2]. Studi lainnya membahas tentang analisa keamanan aset informasi pada Institut Teknologi ABC Surabaya, hasil dari penelitian ini yaitu Institut Teknologi ABC Surabaya memiliki asset kerentanan sehingga membutuhkan pengelolaan keamanan lebih ekstra, selain itu dalam membuktikan bahwa metode OCTAVE allegro dan FMEA efektif dalam melakukan manajemen informasi dan gambaran terhadap risiko [3]. Studi lainnya mengulas tentang Pengelolaan risiko TI pada jaringan komputer dan fasilitas pendukung Dinustek dan PSI menggunakan OCTAVE dan FMEA, hasil dalam penelitian ini aset kritis yang memiliki level Risk Priority Number yang tinggi seperti “Sangat Tinggi” dan “Tinggi” adalah yang harus diberi perhatian lebih, setelah itu membagi perhatiannya dengan risiko yang berlevel dibawahnya [4]. Berdasarkan studi literatur tersebut menjadi dasar acuan dalam analisis keamanan website Dinas Perhubungan Provinsi Jawa Timur.

Pada artikel ini, akan mengidentifikasi, menganalisis, dan juga mengurangi potensi dari beberapa kegagalan dan juga risiko pada sebuah *website* milik instansi pemerintahan yaitu Dinas Perhubungan (Dishub) provinsi Jawa Timur. Dalam artikel ini menggunakan metode OCTAVE Allegro dan FMEA, metode ini digunakan dalam artikel ini karena berfokus pada aset informasi yang mencakup dari identifikasi kegagalan, menilai tingkat keparahan, kemungkinan yang terjadi, dan juga mendeteksi dari setiap kegagalan yang terjadi dengan mengembangkan suatu perbaikan yang sesuai untuk meminimalisir risiko [5]. Kedua metode ini kerap digunakan secara bersama untuk saling melengkapi dalam manajemen risiko dan juga membantu sebuah organisasi atau perusahaan dalam mengoptimalkan kinerja pada sistem. Dengan adanya identifikasi permasalahan tersebut, dapat memiliki tujuan untuk memberikan rekomendasi mitigasi risiko yang akurat dengan hasil identifikasi yang sesuai dengan harapan dan tujuan organisasi atau perusahaan pada layanan website Dinas Perhubungan (Dishub) Provinsi Jawa Timur [6].

2. METODOLOGI

Metodologi merupakan bagian penting dari penelitian ataupun artikel. Pada Gambar 1, metodologi menjelaskan kerangka kerja dan alur dari artikel ini secara sistematis. Dimulai dari tahapan Studi Literatur dan Observasi, Identifikasi Masalah, hingga dapat menarik Kesimpulan.



Gambar 1. Metodologi

2.1 Studi Literatur Dan Observasi

Pada artikel ini, tahap pertama yaitu tahapan studi literatur dan observasi yang bertujuan untuk pengumpulan informasi dan mendalami teori penelitian sebelum melakukan analisis keamanan pada aset informasi. Dalam studi literatur, menelaah lebih lanjut landasan teoritis mengenai sistem manajemen keamanan website dan juga memahami bagaimana metodologi yang digunakan pada artikel ini yaitu metode OCTAVE dan FMEA. Tahapan observasi ini bertujuan untuk mengamati aspek-aspek penting yang berkaitan dengan keamanan website Dinas Perhubungan Provinsi Jawa Timur untuk memahami dan meneliti lebih lanjut mengenai praktik keamanan yang telah dilakukan.

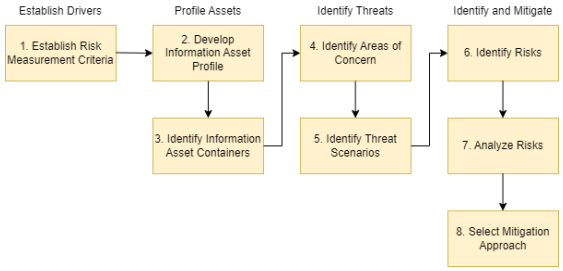
2.2 Identifikasi Permasalahan

Pada website Dinas Perhubungan Provinsi Jawa Timur, ditemukan adanya ancaman *cybercrime* yang dapat mengganggu keberlangsungan kinerja dari dinas tersebut. Oleh karena itu, tujuan dari artikel ini adalah untuk mengevaluasi risiko keamanan pada *website* resmi Dinas Perhubungan Provinsi Jawa Timur dan menyelidiki dampak negatif dan gangguan yang timbul akibat tindakan *cybercrime*, serta mengidentifikasi solusi yang efektif untuk menjaga keberlangsungan instansi.

2.3 Framework Dan Area Keamanan Sistem Informasi

2.3.1 OCTAVE ALLEGRO

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) merupakan sebuah metode yang digunakan untuk melakukan penilaian dan perencanaan strategi keamanan informasi berdasarkan risiko. OCTAVE Allegro adalah metode yang difokuskan pada aset informasi, dengan menggunakan pendekatan workshop-style dan metode kolaboratif yang melibatkan organisasi atau perusahaan. Kerangka kerja OCTAVE digunakan untuk menganalisis dan memantau proses pengelolaan risiko keamanan informasi di sebuah organisasi, dengan tujuan mengurangi kemungkinan terjadinya ancaman dan menemukan langkah-langkah mitigasi untuk menghadapi ancaman yang muncul [7].



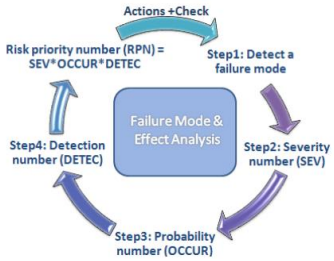
Gambar 2. Gambar Tahapan dan Langkah OCTAVE

Gambar 2 menunjukkan 4 tahap utama dan 8 langkah dalam metode OCTAVE. Tahap pertama, *Establish Drivers*, berfokus pada pengembangan standar pengukuran risiko untuk meningkatkan pengembangan organisasi. Tahap kedua, *Profile Assets*, melibatkan pengembangan profil aset dan identifikasi kontainer aset. Tahap ketiga, *Identify Threats*, bertujuan untuk mengidentifikasi ancaman yang ada pada aset informasi dan menyusun skenario ancaman secara terstruktur. Tahap terakhir, *Identify and Mitigate*, melibatkan identifikasi dan analisis risiko berdasarkan informasi ancaman dan menemukan langkah-langkah mitigasi risiko. Metode FMEA digunakan untuk

menganalisis dan menilai dampak risiko aset informasi, serta menentukan nilai RPN (*Risk Priority Number*) dari aset kritis [3].

2.3.2 FMEA

FMEA (*Failure Mode and Effect Analysis*) ialah metode pendekatan yang dapat digunakan untuk menganalisis risiko yang mencakup potensi kegagalan pada sistem, dan potensi yang teridentifikasi akan dikelompokan berdasarkan level besarnya potensi pada kegagalan dan efeknya pada prosesnya. Berikut pada Gambar 3 merupakan alur tahapan proses FMEA [6].



Gambar 3. Tahapan Proses FMEA

Pada tahapan pertama yaitu mendeteksi kegagalan dimana proses identifikasi pada kegagalan yang dilakukan dengan memberikan nilai pada tingkat kegagalan tersebut yang ada pada tahapan kedua, ketiga, dan keempat dimana dapat dikelompokan berdasarkan Tingkat Keparahan (*Severity*), Tingkat Probabilitas Kejadian (*Occurrence*), dan Tingkat Kemampuan Deteksi (*Detection*). Setelah menentukan *SEV*, *OCCUR*, dan *DETEC* maka ketiga komponen tersebut dikalikan lalu dapat dihasilkan nilai RPN tersebut.

a. *Severity Number* atau yang disebut SEV (Tingkat Keparahan) untuk mengukur tingkat keparahan yang dirasakan pengguna dari efek kegagalan (risiko) tersebut yang disajikan pada Tabel 1.

Tabel 1. Skala Tingkat Keparahan

Dampak	Kriteria	Peringkat
Berbahaya (Tanpa Peringatan)	Melukai pekerja/pihak ketiga/*customer*	10
Berbahaya (Tanpa Peringatan)	Kegiatan yang tidak diberi izin oleh perusahaan	9
Sangat Tinggi	Kesalahan operasional	8
Tinggi	Adanya komplain dari pihak ketiga/*customer*	7
Sedang	Perusahaan mengalami kerugian	6
Rendah	Penurunan kinerja pekerja	5
Sangat Rendah	Hanya sedikit kerugian	4
Minor	Masalah kecil yang dapat diatasi tanpa kehilangan apapun	3
Sangat Minor	Tanpa disadari dan berdampak kecil pada kinerja	2
Tidak Berdampak	Tanpa disadari dan tidak berdampak pada kinerja	1

b. *Probability Number* atau yang disebut OCCUR (Tingkat Kejadian) untuk memperkirakan probabilitas penyebab kemungkinan terjadinya risiko dan akan muncul nilai modus dari risiko yang terjadi dan disajikan pada Tabel 2.

Tabel 2. Skala Tingkat Kejadian

Probabilitas Risiko	Periode Waktu	Peringkat
Sangat Tinggi	Setiap hari lebih dari sekali	10
Tinggi (Kegagalan tinggi yang harus dihadapi)	Satu kali dalam empat hari	9
Tinggi (Proses yang beberapa kali mengalami kegagalan sebelumnya)	Seminggu sekali	8
Proses yang sering mengalami kegagalan	Sebulan sekali	7
Moderate (Proses yang sebelumnya sering mengalami kegagalan)	Satu kali setiap 3 bulan	6

Proses sebelumnya yang tidak terlalu sering mengalami kegagalan	Satu kali setiap 6 bulan	5
Kegagalan yang pernah terjadi dalam proporsi kecil	Setahun sekali	4
Rendah (Kegagalan yang terisolasi dengan proses serupa)	Satu kali dalam 1-3 tahun	3
Sangat rendah (Kegagalan yang proses terjadinya hampir sama)	Satu kali dalam 3-6 tahun	2
Remote (Kegagalan yang tidak mungkin terjadi)	Satu kali dalam 6-100 tahun	1

c. *Detection Number* atau yang disebut DETECT (Tingkat Kemampuan Deteksi) untuk mengukur sejauh mana peluang risiko kegagalan dapat dideteksi yang disajikan pada Tabel 3.

Tabel 3. Skala Tingkat Kemampuan Deteksi

Dampak	Kriteria	Peringkat
Hampir tidak terjadi	Kegagalan tidak bisa dideteksi oleh sistem pengontrol	1
Sangat kecil terjadi	Kemungkinan pengontrol menemukan potensi kegagalan sangat kecil	2
Kecil terjadi	Kemungkinan pengontrol menemukan potensi kegagalan hanya beberapa kali atau jarang	3
Sangat rendah terjadi	Kemungkinan pengontrol mendeteksi kegagalan sangat rendah	4
Rendah terjadi	Peluang pengontrol mendeteksi terjadinya kegagalan rendah	5
Sedang / tengah	Kemungkinan pengontrol dapat mendeteksi terjadinya kegagalan dalam tingkatan sedang	6
Cukup tinggi terjadi	Peluang pengontrol mendeteksi terjadinya kegagalan cukup tinggi	7
Tinggi terjadi	Peluang pengontrol mendeteksi terjadinya kegagalan tinggi	8
Sangat tinggi terjadi	Kemungkinan pengontrol dapat mendeteksi terjadinya kegagalan sangat tinggi	9
Hampir pasti terjadi	Dalam proses tidak terjadi kegagalan karena telah datasi oleh sistem solusi yang ada	10

Ketiga hal tersebut kemudian dihitung untuk mendapatkan nilai prioritas risiko yang merupakan *Risk Priority Number* (RPN). RPN digunakan untuk mengukur risiko dari kegagalan dan menentukan prioritas tindakan mitigasi. Skala RPN bisa dihitung menggunakan persamaan dari ketiga variabel berikut ini:

$$RPN = Severity \times Occurence \times Detection \quad \ldots\ldots(1)$$

Setelah mendapatkan skor nilai dari skala RPN, hasil tersebut dikelompokkan menjadi 5 tingkatan yang dapat dilihat pada Tabel 4.

Tabel 4. Skala RPN

Skala RPN	Level Risiko
200>	Sangat Tinggi
151 - 200	Tinggi
101 - 150	Sedang
51 - 100	Rendah
0 - 50	Sangat Rendah

Dari hasil perhitungan tersebut maka akan diperoleh hasil yang digunakan untuk menentukan tingkat risiko [4].

2.3.3 Area Keamanan Sistem Informasi

Dalam artikel ini, terdapat beberapa area keamanan sistem informasi yang perlu diperhatikan. Aset informasi tersebut meliputi komponen-komponen penting dalam sistem informasi yang mencakup *Hardware, Software,* Data, *Network*, dan *People*. keseluruhan keamanan sistem

informasi melibatkan langkah-langkah yang diperlukan untuk melindungi aset informasi dalam penggunaan dan pengoperasian sistem tersebut.

2.4 Instrumen Penelitian

Pengumpulan data dilakukan dengan teknik wawancara yang dilakukan dapat digunakan sebagai acuan untuk menunjang artikel. Dalam artikel ini dilakukan wawancara terhadap pihak yang terkait dengan website Dinas Perhubungan Provinsi Jawa Timur untuk mengumpulkan data yang diperlukan, dengan tujuan mendapatkan uraian terkait dengan kegagalan yang terjadi dan penyebabnya. Pada tahap wawancara menggunakan acuan kerangka kerja OCTAVE digunakan untuk mendapatkan sebuah data dan informasi yang nantinya dapat digunakan untuk mendefinisikan penyebab ancaman, mengidentifikasi pada aset organisasi kritis dan melakukan evaluasi pada keamanan pada organisasi.

2.5 Pengumpulan Data

Setelah pengumpulan data, data tersebut diolah menggunakan metode OCTAVE dan FMEA. OCTAVE digunakan sebagai pendekatan kualitatif yang efisien, sementara FMEA digunakan sebagai pendekatan kuantitatif. Data yang dikumpulkan dan dianalisis digunakan untuk memprioritaskan perbaikan, mengidentifikasi risiko dan ancaman pada website resmi Dinas Perhubungan Provinsi Jawa Timur berdasarkan evaluasi dampak risiko. Metode FMEA digunakan untuk mengevaluasi tingkat risiko seperti mode kegagalan, tingkat keparahan, dan deteksi kegagalan dengan menggunakan nilai RPN risiko. Artikel ini menggunakan kombinasi pendekatan kualitatif dan kuantitatif untuk memperoleh pemahaman komprehensif terkait risiko keamanan dan langkah-langkah mitigasinya secara keseluruhan [5].

3. HASIL DAN PEMBAHASAN

3.1 Identifikasi Ancaman Aset

Dalam artikel ini, langkah pertama yang dilakukan ialah studi literatur dan identifikasi masalah. Teknik pengumpulan data pada artikel ini menggunakan wawancara dengan pihak yang terkait secara langsung menangani *website* https://dishub.jatimprov.go.id/ terkait dengan kondisi aset informasi yang ada pada Dinas Perhubungan Jawa Timur.

Table 5. Aset Informasi

Aset Informasi	Kategori Aset
PC *Server* Printer Laptop	*Hardware*
Website https://dishub.jatimprov.go.id/	*Software*
Data PPID Data Laporan Sakip Data Informasi Berita	Data
Router *Access Point*	*Network*
Pranata Ahli Komputer	*People*

Pada Tabel 5 dapat diketahui bahwa dari hasil wawancara terdapat 11 aset informasi yang telah dikategorikan kedalam 5 aset yaitu; *Hardware*, *Software*, Data, *Network dan People*. Langkah selanjutnya yaitu mengidentifikasi terkait kebutuhan keamanan pada setiap aset dari hasil wawancara sebelumnya. Dalam menentukan kebutuhan keamanan, ada tiga kategori prinsip dasar keamanan informasi yang menjadi acuan, yaitu *CIA Triad* (*Confidentiality*, *Integrity*, *Availability*) yang terdokumentasikan dalam Tabel 6.

Tabel 6. CIA

Aset	*Confidentiality*	*Integrity*	*Availability*
Hardware	Pembatasan akses yang hanya diperuntuk untuk Pranata ahli komputer.	Penjagaan terkait keamanan akses dari	*Controller* terkait pengadaan alat dan barang.

	Pengadaan CCTV guna untuk pemantauan keamanan fisik. Penerapan kata sandi atau PIN pada *hardware.*	orang yang tidak berkepentingan.	Akses *hardware* selalu tersedia dalam berbagai situasi.
Software	Pemberian hak akses berdasarkan yang bersangkutan. Penerapan kebijakan privasi data sensitif dalam software.	Pemeriksaan keaslian proses data oleh software. Pencegahan modifikasi secara illegal.	Pemantauan ketersediaan pemulihan software. Pengelolaan prosedur pemulihan insiden.
Data	Perlindungan kerahasiaan informasi data. Penguncian untuk mengakses data.	Penerapan verifikasi dalam pengubahan data.	Pencadangan backup and recovery data secara teratur setiap bulan.
Network	Penggunaan firewall dan sistem deteksi intrusi (IDS) untuk mencegah akses yang mencurigakan.	Pemantauan perubahan tidak sah pada konfigurasi jaringan.	Pengawasan gangguan ketersediaan jaringan. Pengadaan perangkat jaringan yang tangguh.
People	Penerapan kebijakan dan prosedur terkait perjanjian informasi perusahaan. Melakukan kontrol akses yang tepat.	Menjalankan prinsip etika profesional. Menerapkan peraturan pelaporan pelanggaran.	Memastikan tanggung jawab pekerja terhadap ketersediaan informasi.

3.2 Identifikasi Penyebab Potensial

Setelah mengetahui terkait kebutuhan keamanan setiap aset. Tahap selanjutnya yaitu identifikasi *Potensial Cause*. Penyebab *potensial cause* ialah timbulnya suatu bahaya yang terjadi dari kerawanan dan ancaman. Identifikasi kerawanan dan identifikasi ancaman adalah suatu aset yang dapat mengancam aset informasi yang dapat dilihat pada Tabel 7.

Tabel 7. Identifikasi Penyebab Potensial

Aset Informasi	Kerawanan	Penyebab	Ancaman
PC	Korsleting Listrik	Tidak adanya pemeliharaan sistem.	Kerusakan pada fasilitas peralatan / media.
Server	Rawannya berbagai informasi yang tersedia pada server.	Minimnya sistem pengamanan perusahaan.	Dapat kehilangan data.
Printer	Kerentanan terhadap kotoran.	Kurangnya pemeliharaan sistem.	Terjadinya pengeroposan pada *hardware.*
Laptop	Terjadi *hang* saat penggunaan.	Penggunaan memori data melampaui batas.	Kinerja server menurun.
Website : https://dishub.jatimprov.go.id/	Terjadinya ahli fungsi admin.	Pembaruan *software* yang terlewat.	Adanya perubahan pada *website.*
Data PPID	Serangan *phishing*	Kelalaian admin dalam pengamanan *software.*	Adanya perubahan pada informasi.
Data Laporan Sakip	Serangan *malware*	Kelalaian admin dalam pemeliharan *software.*	Adanya perubahan pada informasi.
Data Informasi Berita	Kebocoran data yang tidak dipublish.	Kelemahan keamanan sistem.	Munculnya data berita yang tidak dipublish.

Router	*Overload* jaringan	Kurangnya mekanisme pemantauan jaringan.	Performa yang buruk dengan kecepatan transfer data yang rendah.
Access Point	Kualitas jaringan kurang baik.	Adanya kerusakan pada saluran kabel.	Kehilangan koneksi
Pranata Ahli Komputer	Meremehkan pengecekan sistem berkala.	Kurangnya kedisiplinan	Terjadinya serangan pada sistem.

3.3 Identifikasi Risiko

Tahapan selanjutnya yaitu identifikasi resiko yang dapat mengancam aset informasi dari Dinas Perhubungan Jawa Timur yang berasal dari *potential cause*. Risiko yang dimaksud ialah suatu kejadian bahaya yang kemungkinan akan terjadi bahkan sering terjadi terhadap aset informasi. Pada Tabel 8 merupakan hasil dari identifikasi risiko pada aset informasi Dinas Perhubungan Jawa Timur.

Tabel 8. Identifikasi Risiko

Aset	Potential Cause	Risiko
Hardware (PC, Server, Printer, Laptop)	Tidak adanya pemeliharaan sistem	Kerusakan pada *hardware.*
	Minimnya sistem pengamanan perusahaan	Pencurian dan kehilangan informasi data penting.
	Penggunaan memori data melampaui batas	Memori data penuh.
Software (Website)	Pembaruan Perangkat Lunak yang Terlewat	Kegagalan perangkat lunak.
Data (Data PPID, Data Laporan Sakip, dan Data Informasi Berita)	Kelalaian admin dalam pengamanan software Kurangnya dalam pemeliharan software Kelemahan keamanan sistem	Serangan hacker
Network (Router dan Access Point)	Kurangnya mekanisme pemantauan jaringan Adanya kerusakan pada saluran kabel	Network failure
People (Pranata Ahli Komputer)	Kurangnya kedisiplinan	Human error

3.4 Penilaian Risiko

Setelah proses identifikasi risiko selesai, langkah berikutnya adalah penilaian risiko. Pada tahap ini dilakukan dengan cara menentukan tingkat atau nilai dari *severity*, *occutance*, dan *detection.* selanjutnya hasil dari penentuan tingkat *severity*, *occutance*, dan *detection* digunakan pada perhitungan rumus RPN (Risk Priority Number) yang nantinya akan menjadi penentuan terhadap prioritas risiko berdasarkan hasil perhitungan RPN yang dapat dilihat pada Table 9.

Table 9. Hasil Perhitungan RPN

Risiko	Penyebab Potensial	SEV	OCC	DEC	RPN	Level
Kerusakan pada hardware	Tidak adanya pemeliharaan sistem	8	3	7	168	Tinggi
Pencurian data kehilangan informasi data penting	Minimnya sistem pengamanan perusahaan	3	3	7	63	Rendah
Memori data penuh.	Penggunaan memori data melampaui batas	5	4	6	120	Sedang

Kegagalan perangkat lunak.	Pembaruan Perangkat Lunak yang Terlewat	8	2	5	80	Rendah
Serangan hacker	Kelalaian admin dalam pengamanan software	5	2	5	50	Sangat Rendah
	Kurangnya dalam pemeliharan software	3	3	5	45	Sangat Rendah
	Kelemahan keamanan sistem	3	2	5	30	Sangat Rendah
Network failure	Kurangnya mekanisme pemantauan jaringan	6	2	8	96	Rendah
Kegagalan dalam jaringan.	Adanya kerusakan pada saluran kabel	3	4	5	60	Rendah
Human error	Kurangnya kedisiplinan	3	4	7	84	Rendah

3.5 Mitigasi Risiko

Setelah melakukan semua tahapan diatas, selanjutnya adalah penentuan dari mitigasi risiko. Hasil dari penilaian risiko pada Table 9, digunakan sebagai acuan peneliti untuk dapat menentukan mitigasi risiko terhadap ancaman aset informasi Dinas Perhubungan Jawa Timur, yang bertujuan untuk kelancaran dalam proses bisnis dan meminimalisir kerugian pada Dinas Perhubungan Provinsi Jawa Timur. Hasil diskusi kelompok dengan pihak terkait terhadap mitigasi risiko ada pada Table 10.

Table 10. Mitigasi Risiko

Aset Informasi	Risiko	Upaya Mitigasi Risiko
Hardware (PC, Server, Printer, Laptop)	Kerusakan pada hardware	Menjadwal secara rutin mengecek terhadap perangkat keras dengan kurun waktu minimal sekali dalam seminggu.
	Pencurian dan kehilangan informasi data penting.	Dengan melakukan enkripsi data.
	Memori data penuh.	Memeriksa redundansi pada *hard disk* (memori) dan menggunakan memori secara tepat dan efisien.
Software (Website)	Kegagalan perangkat lunak.	Mengecek pembaruan perangkat lunak dengan versi terbaru secara teratur.
Data (Data PPID, Data Laporan Sakip, Data Informasi Berita)	Serangan Hacker	Memasang firewall dan sistem deteksi intrusi (IDS) untuk perlindungan data.
Network (Router, Access Point)	Network failure	Memantau aktivitas jaringan untuk mendeteksi aktivitas mencurigakan.
People (Pranata Ahli Komputer)	Human error	Memberi kesadaran atau sosialisasi pada setiap pekerja.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis dan artikel yang telah dilakukan, dapat disimpulkan bahwa manajemen keamanan website Dinas Perhubungan Provinsi Jawa Timur yang menggunakan metode OCTAVE ALLEGRO dan FMEA sudah memenuhi tujuan dari artikel yang mana telah menghasilkan nilai cukup baik dalam manajemen keamanan websitenya, tetapi masih perlu

beberapa improvisasi di bagian prosedur pengecekan rutin agar tidak menghindari terjadinya serangan *cyber*. Serta dihasilkan penilaian risiko yang paling tinggi terdapat pada level tinggi, memiliki nilai RPN sebesar 168 pada tidak adanya pemeliharaan sistem, dan pada level sangat rendah yang merupakan risiko yang paling rendah, memiliki nilai RPN sebesar 30 pada kelemahan keamanan sistem. Dengan kata lain, risiko keamanan pada website Dinas Perhubungan Provinsi Jawa Timur sangat jarang terjadi risiko kerawanan dan ancaman, meskipun jarang dilakukan pengecekan bila tidak terjadi hal-hal yang mencurigakan.
Untuk penelitian berikutnya, disarankan untuk memperluas metode pengukuran dengan memasukkan alat ukur tambahan seperti *Basic Risk Management Facilitation Method*, FTA *(Fault Tree Analysis*), dan HACCP (*Hazard Analysis Critical Control Point*). Dengan menggabungkan alat ukur ini, diharapkan hasil penelitian akan menjadi lebih komprehensif dan menyeluruh dalam menganalisis aspek-aspek pengelolaan risiko dalam konteks yang diteliti. Selain itu penambahan subjek wawancara perlu ditambahkan pada penelitian sejenis seperti ini agar dapat memperoleh pemahaman yang lebih mendalam dan hal ini dapat memberikan perspektif yang beragam dan mendalam, serta memperkaya analisis dan temuan penelitian.

5. DAFTAR RUJUKAN

[1] I. Chintya, "Pengaruh Pemanfaatan Teknologi Informasi dan Sisitem Pengendalian Intern Pemerintah Terhadap Kinerja Instansi Pemerintah di Kota Solok (Studi pada SKPD Kota Solok)," *J. Akunt.*, vol. 3, no. 1, pp. 1–14, 2015, [Online]. Available: http://ejournal.unp.ac.id/students/index.php/akt/article/view/1643

[2] R. J. Gagas, I. Syah, and F. Febryanto, "Analisis, Evaluasi, Dan Mitigasi Risiko Aset Teknologi Informasi Menggunakan Framework Octave Dan Fmea (Studi Kasus: Unit Pengelola Teknis Teknologi Informasi Dan Komunikasi Universitas Xyz)," *J. Khatulistiwa Inform.*, vol. 9, no. 2, pp. 121–133, 2021, doi: 10.31294/jki.v9i2.11368.

[3] A. Pakarbudi, D. T. Piay, D. Nurmadewi, and A. Rachman, "Analisa Efektivitas Metode Octave Allegro dan Fmea Dalam Penilaian Risiko Aset Informasi Pada Institusi Pendidikan Tinggi," *JURIKOM (Jurnal Ris. Komputer)*, vol. 10, no. 2, p. 488, 2023, doi: 10.30865/jurikom.v10i2.5950.

[4] S. Gunawan and K. Yupie, "Mitigasi risiko aset dan komponen teknologi informasi berdasarkan kerangka kerja OCTAVE dan FMEA pada Universitas Dian Nuswantoro," *J. Inf. Syst.*, vol. 9, no. 2, pp. 513–522, 2017.

[5] M. Data, G. Ramadhan, and K. Amron, "Analisis Availabilitas dan Reliabilitas Multi-Master Database Server Dengan State Snapshot Transfers (SST) Jenis Rsync Pada MariaDB Galera Cluster," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 1, p. 69, 2017, doi: 10.25126/jtiik.201741288.

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

[7] V. A. Prabawati, A. Rachmadi, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan Kerangka Kerja OCTAVE-S Pada Unit Pengelola Sistem Informasi Dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 3, pp. 2829–2836, 2019.