Analisis Risiko Keamanan Sistem Informasi DP3AK Provinsi Jawa Timur menggunakan Metode Octave dan FMEA

Dianita Puspitasari*[1], Eristya Maya Safitri[2], Aidah Maryam Barmin[3], Imamah Nur Fadlilah[4]
Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur
e-mail: [1]dianitapuspitasari27@gmail.com, [2]maya.si@upnjatim.ac.id, [3]aidahbarmin01@gmail.com, [4]imamahnf123@gmail.com
*Penulis Korespondensi

Diterima: 16 Juni 2023; Direvisi: 25 September 2023; Disetujui: 03 Juli 2024

Abstrak

Dinas Pemberdayaan Perempuan, Perlindungan Anak, dan Kependudukan (DP3AK) Provinsi Jawa Timur memanfaatkan teknologi informasi untuk menjalankan aktivitasnya. Namun, seiring dengan pemanfaatan teknologi, keamanan sistem informasi (SI) menjadi krusial, terutama dalam melindungi data sensitif yang dimiliki DP3AK. Ancaman terhadap keamanan SI dapat berdampak signifikan pada operasional dan reputasi organisasi. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis risiko keamanan SI yang dihadapi DP3AK, sehingga langkah-langkah mitigasi yang tepat dapat diambil. Penelitian ini menerapkan kombinasi metode Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) dan Failure Mode and Effects Analysis (FMEA) untuk mengevaluasi risiko. Metode OCTAVE membantu mengidentifikasi aset-aset kritis, ancaman, dan kerentanan, sementara FMEA digunakan untuk menganalisis potensi kegagalan dan dampaknya. Dari 13 aset yang diteliti, ditemukan 3 aset dengan tingkat risiko tinggi, 5 aset dengan risiko sedang, 4 aset dengan risiko rendah, dan 1 aset dengan risiko sangat rendah. Aset-aset berisiko tinggi tersebut meliputi aplikasi e-KembangPernik dengan risiko hardware failure, aplikasi Super Sinden dengan risiko software failure, dan data administrasi kependudukan provinsi Jawa Timur dengan risiko backup data failure. Hasil penelitian ini memberikan informasi penting bagi DP3AK untuk memprioritaskan upaya mitigasi pada aset-aset kritis. Penelitian ini juga berkontribusi pada peningkatan kesadaran akan pentingnya keamanan SI di lingkungan pemerintahan dan memberikan rekomendasi praktis untuk pengelolaan risiko yang lebih baik.

Kata kunci: *Keamanan Sistem Informasi, Analisis Risiko, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), FMEA (Failure Mode and Effects Analysis)*

Abstract

The East Java Province's Office of Women's Empowerment, Child Protection, and Population (DP3AK) leverages information technology to facilitate its operations. However, with this technological reliance, information system (IS) security becomes paramount, especially for safeguarding DP3AK's sensitive data. Threats to IS security can significantly impact the organization's operations and reputation. This research aims to identify and analyze the IS security risks faced by DP3AK, enabling the implementation of appropriate mitigation measures. This study employs a combined methodology of Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and Failure Mode and Effects Analysis (FMEA) for risk

assessment. OCTAVE facilitates the identification of critical assets, threats, and vulnerabilities, while FMEA is utilized to analyze potential failures and their consequences. From the 13 assets examined, 3 were identified as high risk, 5 as medium risk, 4 as low risk, and 1 as very low risk. The high-risk assets include the e-KembangPernik application (hardware failure risk), the Super Sinden application (software failure risk), and the East Java provincial population administration data (backup data failure risk). These findings provide crucial information for DP3AK to prioritize mitigation efforts on critical assets. By understanding these risks, DP3AK can develop more effective security strategies, enhance the protection of sensitive data, and ensure operational continuity. This research contributes to raising awareness of the importance of IS security within government environments and offers practical recommendations for improved risk management.

***Keywords**: Information System (IS) Security, Risk Assessment, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), FMEA (Failure Mode and Effects Analysis)*

1. PENDAHULUAN

Di era digital ini, Dinas Pemberdayaan Perempuan, Perlindungan Anak, dan Kependudukan (DP3AK) Provinsi Jawa Timur telah memanfaatkan teknologi informasi untuk meningkatkan efektivitas dan efisiensi layanannya. DP3AK, sebagai institusi pemerintah yang bertanggung jawab merancang dan melaksanakan kebijakan terkait pemberdayaan perempuan, perlindungan anak, dan pengendalian penduduk di Jawa Timur [1], menggunakan berbagai sistem informasi untuk mendukung aktivitasnya. Beberapa sistem tersebut antara lain Aplikasi Super Sinden, Aplikasi e-KembangPernik dan Aplikasi Siak Terpusat. Pemanfaatan teknologi informasi ini memungkinkan DP3AK untuk memberikan layanan yang lebih baik, cepat, dan mudah diakses oleh masyarakat.

Namun dibalik pemanfaatan dan pengelolaan sistem informasi, terdapat risiko yang harus dihadapi DP3AK Provinsi Jawa Timur ini dalam penerapan teknologinya. Menurut David Vose risiko merujuk pada konsekuensi negatif yang timbul akibat kemungkinan terjadinya suatu peristiwa yang tidak dapat diprediksi terhadap pencapaian tujuan organisasi. [2]. Risiko tersebut dapat berupa berbagai ancaman yang dapat berpengaruh terhadap aktivitas perusahaan tersebut. Salah satu risiko yang dapat dialami oleh DP3AK provinsi Jawa Timur adalah ancaman terhadap keamanan SI yang digunakan. Deskripsi tentang keamanan sistem informasi mencakup penggunaan berbagai mekanisme dengan tujuan untuk melindungi sistem tersebut dari *threats* yang dapat menyebabkan dampak negatif terhadap keamanan data informasi dan juga melibatkan pelaku-pelaku yang bertujuan menjaga keamanan sistem. [3]. Keamanan sistem informasi DP3AK Provinsi Jawa Timur memiliki peran yang vital dalam melindungi informasi sensitif dan penting, seperti data pribadi penduduk, data terkait anak - anak yang memerlukan perlindungan, dan data yang berkaitan dengan program pemberdayaan perempuan. Maka dari banyaknya data yang ada tersebut menimbulkan ancaman yang dihadapi selama penggunaan sistem berupa pengelolaan data yang kurang di manajemen, hal tersebut dapat mempengaruhi performa dari dinas tersebut.

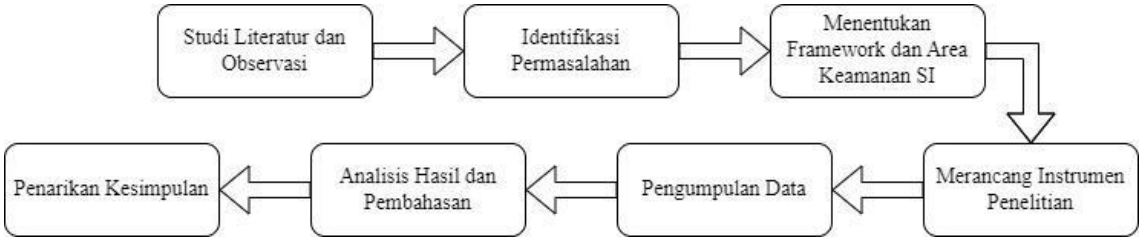
Berdasarkan permasalahan yang dialami tersebut maka perlu adanya langkah awal untuk mengatasi risiko tersebut. Langkah tersebut dapat diawali dengan identifikasi aset kritis dan risiko aset kritis yang dimiliki Dinas dengan menggunakan metode OCTAVE. Langkah selanjutnya yaitu melakukan penilaian risiko terhadap aset yang telah diketahui sebelumnya dan menentukan mitigasi terhadap risiko tersebut dengan menggunakan FMEA. Metode OCTAVE dan FMEA ini cocok digunakan untuk mengetahui risiko yang dapat menyerang aset yang dimiliki oleh suatu perusahaan.

Oleh karena itu, tujuan dari penelitian ini adalah untuk mengidentifikasi risiko-risiko keamanan SI apa saja yang akan dihadapi dinas dalam menerapkan sistem informasi untuk menjalankan aktivitas - aktivitas penting dalam perusahaan. Dan dari analisis risiko tersebut

DP3AK Provinsi Jawa Timur dapat terus memperkuat keamanan sistem informasi yang dimilikinya. Hal ini akan memastikan bahwa DP3AK Provinsi Jawa Timur dapat menjalankan tugasnya secara efektif dan melindungi informasi yang sensitif dan penting dengan baik.

2. METODE PENELITIAN

Bagian ini akan menguraikan tentang metode dan tahapan yang digunakan dalam penelitian. Tahapan - tahapan tersebut terdiri dari studi literatur dan observasi, identifikasi permasalahan, menentukan framework dan area keamanan sistem informasi, merancang instrumen penelitian, pengumpulan data, analisis hasil dan pembahasan, serta penarikan kesimpulan.



Gambar 1. Metode penelitian

2.1. Studi literatur dan Observasi

Tahapan pertama dalam penelitian ini adalah melakukan studi literatur dan observasi. Studi literatur digunakan untuk memperoleh pemahaman yang komprehensif tentang topik penelitian, mengidentifikasi landasan teori yang ada, serta mengeksplorasi penelitian terdahulu yang telah dilakukan. Studi literatur diperoleh dari media tertulis. Penelitian ini melakukan observasi secara tatap muka serta melakukan wawancara dengan dinas terkait. Data yang diperoleh dari wawancara akan dipergunakan untuk menyusun penelitian ini.

2.2. Identifikasi Permasalahan

Keamanan sistem informasi DP3AK Provinsi Jawa Timur memiliki peran yang vital dalam melindungi informasi sensitif dan penting, seperti data pribadi penduduk, data terkait anak - anak yang memerlukan perlindungan, dan data yang berkaitan dengan program pemberdayaan perempuan. Dengan banyaknya informasi yang ada, membuat keamanan sistem informasi dinas memiliki berbagai ancaman, diantaranya yaitu pengelolaan data yang kurang di manajemen, penyalahgunaan hak akses, terserang virus dan sebagainya. Maka dari itu penting untuk memahami risiko keamanan SI apa saja yang akan dihadapi dinas dalam menerapkan sistem informasi untuk menjalankan aktivitas - aktivitas penting dalam perusahaan.

2.3. Menentukan Framework dan Area Keamanan SI

Framework yang digunakan yaitu menggunakan OCTAVE dan FMEA. Metode OCTAVE yaitu suatu pendekatan dan teknik yang digunakan sebagai pendekatan untuk mengenali, menganalisis, dan memantau manajemen risiko keamanan informasi dengan fokus pada identifikasi risiko [4]. Sedangkan Metode FMEA yaitu suatu metode untuk mengenali semua kemungkinan kegagalan yang dapat terjadi dalam perancangan atau proses produksi suatu produk, serta mengkaji konsekuensi dari setiap kegagalan tersebut [5]. Kedua metode tersebut sangat cocok digunakan untuk mengidentifikasi risiko dan level tingkat risiko yang ada pada suatu perusahaan. Untuk area keamanan sistem informasi yang diidentifikasi meliputi aset penting seperti perangkat keras (*hardware*), perangkat lunak (*software*), jaringan (*network*), data, dan pengguna (*people*).

2.4. Merancang Instrumen Penelitian

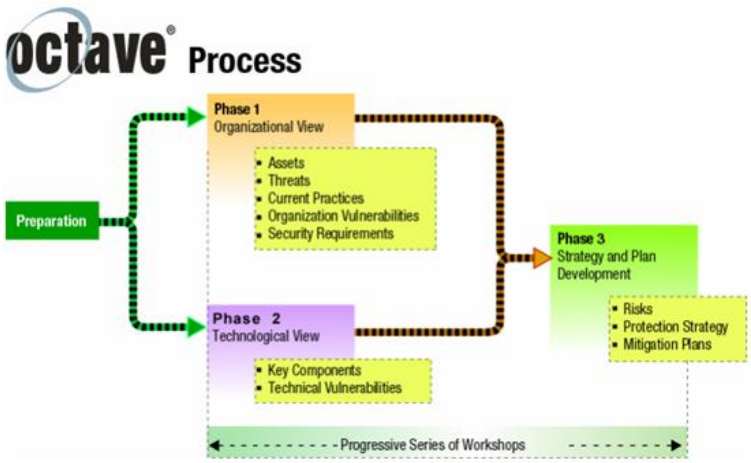
Pada tahapan ini dilakukan proses merancang instrumen yang digunakan dalam proses wawancara. Kerangka kerja metode OCTAVE dapat digunakan sebagai acuan dalam pembuatan instrumen untuk mendapatkan informasi dan data yang diperlukan saat proses wawancara. Instrumen tersebut dapat berupa aset apa saja yang dimiliki dinas, ancaman, gangguan atau risiko yang pernah terjadi, penyebab terjadinya risiko, seberapa sering risiko terjadi serta cara yang dilakukan dinas untuk menangani risiko tersebut.

2.5. Pengumpulan Data

Data yang telah didapatkan dari proses wawancara akan diolah menjadi sebuah informasi. Data tersebut terdiri dari data yang bersifat kualitatif dan data kuantitatif. Data kualitatif akan diolah menggunakan metode OCTAVE, karena sesuai dengan kegunaannya yaitu untuk mengidentifikasi, menganalisis aset dan risiko yang ada. Selanjutnya setelah data kualitatif diolah akan menghasilkan data berupa data kuantitatif berupa nilai risiko dari setiap aset yang ada. Proses pengolahan data ini menggunakan tahapan - tahapan pada metode FMEA.

2.6. Metode OCTAVE

Metode OCTAVE digunakan untuk mengenali, menganalisis dan mengawasi pengelolaan risiko keamanan informasi berdasarkan pengidentifikasian risiko. Dalam penggunaan metode OCTAVE, memiliki tiga tahapan yang dapat digunakan untuk menjalankan suatu penelitian.



Gambar 2. Alur Metode OCTAVE [6]

Berdasarkan gambar 2, metode OCTAVE terdiri dari beberapa tahap meliputi: tahap (1) melakukan identifikasi terhadap aset yang dianggap kritis dan memiliki potensi terhadap ancaman. Diawali dengan mengelompokkan aset yang krusial bagi organisasi. Tahap (2) melakukan identifikasi kelemahan teknologi yang digunakan organisasi dengan mengidentifikasi elemen inti dan kerentanan terhadap teknologi terkait. Tahap (3) mengidentifikasi risiko yang terkait dengan setiap aset yang telah diidentifikasi, merumuskan strategi perlindungan, dan merencanakan langkah mitigasi risiko.

2.7. Metode FMEA

Metode FMEA berguna untuk memberikan nilai pada risiko yang telah diidentifikasi oleh metode OCTAVE. Tahapan penilaian metode FMEA [6] terdiri dari: tahap (1) Severity (S) atau tingkat keparahan merupakan evaluasi sejauh mana efek dari kemungkinan kegagalan yang potensial terjadi dari tingkat 1-10, dengan 1 menjadi nilai terendah. Skala tingkat keparahan dapat dilihat dalam tabel 1.

Tabel 1. Skala tingkat keparahan

Dampak	Kriteria	Peringkat
Berbahaya: Tidak Adanya Peringatan	Melukai pekerja/pihak ketiga/customer	10
Berbahaya: Tidak Adanya Peringatan	Kegiatan yang tidak diperbolehkan	9
Sangat Tinggi	Kegagalan dalam memanfaatkan peralatan yang tersedia	8
Tinggi	Melahirkan aduan dari pihak ketiga atau pelanggan	7
Sedang	Melahirkan kerugian bagi badan usaha	6
Rendah	Melahirkan penurunan produktivitas dari karyawan	5
Sangat Rendah	Melahirkan sedikit kerugian	4
Minor	Melahirkan gangguan minor yang dapat diselesaikan tanpa mengalami kerugian	3
Sangat Minor	Tanpa sadar dan memiliki dampak minor terhadap kinerja	2
Tidak Berdampak	Tanpa sadar dan tidak berpengaruh terhadap kinerja	1

Tahap (2) Occurrence (O) atau kejadian, merupakan frekuensi kegagalan pada suatu aset diberikan pada tingkat 1-10, dengan 1 sebagai nilai terendah. Skala tingkat kejadian dapat dilihat dalam tabel 2.

Tabel 2. Skala tingkat kejadian

Dampak	Kriteria	Peringkat
Sangat Tinggi	Lebih dari satu kali tiap harinya	10
Tinggi : tingkat kegagalan tidak terelakan	Dalam 4 hari, kegagalan sekali	9
Tinggi: Secara umum, berkaitan dengan prosedur yang telah terjadi sebelumnya mengalami kegagalan berulang	Dalam seminggu, mengalami kegagalan sekali	8
Proses yang sering kali gagal	Dalam sebulan, kegagalan sekali	7
Moderat: Proses yang sebelumnya sering mengalami kegagalan	Setiap 3 bulan, mengalami kegagalan sekali	6
Cukup jarang: Proses sebelumnya mengalami kegagalan, tetapi tidak terlalu sering	Setiap 6 bulan, mengalami kegagalan sekali	5
Terbatas: Kegagalan pernah terjadi, tetapi tidak dalam skala yang besar	Dalam setahun, mengalami kegagalan sekali	4
Rendah : Kegagalan yang terjadi secara terbatas dan terisolasi terkait dengan proses yang serupa	Dalam 1-3 tahun, mengalami kegagalan sekali	3
Sangat rendah: Kegagalan hanya terkait dengan proses yang sangat sebanding	Dalam 3-6 tahun, mengalami kegagalan sekali	2
Jarang sekali: Kegagalan tidak mungkin terjadi, dan tidak ada kegagalan sebelumnya terkait dengan proses yang sebanding	Dalam 6-100 tahun, mengalami kegagalan sekali	1

Tahap (3) Detection (D) merupakan evaluasi terhadap probabilitas deteksi penyebab kegagalan suatu aset diberikan pada tingkat 1-10, dengan 1 sebagai nilai tertinggi. Skala tingkat deteksi dapat dilihat dalam tabel 3.

Tahap (4) Risk Priority Number (RPN) merupakan hasil prioritas risiko yang didapat dari perkalian (x) antara Severity, Occurrence, dan Detection dengan rumus RPN = S x O x D. Nilai RPN dapat dilihat dalam tabel 4.

Tabel 3. Skala tingkat deteksi

Dampak	Kriteria	Peringkat
Hampir tidak mungkin	Pengendalian tidak mampu mengidentifikasi kegagalan	1
Sangat kecil	Sangat tidak mungkin pengendalian akan menemukan potensi kegagalan	2
Kecil	Jarang kemungkinan pengendalian akan menemukan potensi kegagalan	3
Sangat rendah	Peluang pengendalian untuk mengenali kesalahan sangat rendah	4
Rendah	Peluang pengendalian untuk mengenali kesalahan rendah	5
Sedang / moderat	Peluang pengendalian untuk mengenali kesalahan sedang	6
Cukup tinggi	Peluang pengendalian untuk mengenali kesalahan cukup tinggi	7
Tinggi	Peluang pengendalian untuk mengenali kesalahan tinggi	8
Sangat tinggi	Peluang pengendalian untuk mengenali kesalahan sangat tinggi	9
Hampir pasti	Tidak mungkin terjadi kesalahan dalam proses karena telah dicegah melalui sistem solusi	10

Tabel 4. Nilai RPN

Level	Nilai RPN
< 51	Very Low
< 101	Low
< 151	Medium
< 201	High
> 200	Very High

2.8. Penarikan Kesimpulan

Pada penelitian ini pengumpulan data yang digunakan yaitu berupa studi literatur pada penelitian terdahulu dan wawancara pada pihak dinas yang terkait. Metodologi yang digunakan pada penelitian ini yaitu metode OCTAVE dan FMEA. Kedua metode tersebut sangat cocok digunakan untuk melakukan identifikasi risiko dan level tingkat risiko yang ada pada suatu perusahaan.

3. HASIL DAN PEMBAHASAN

Pada hasil dan pembahasan akan menjelaskan mengenai identifikasi aset kritis, ancaman dan kerentanan terhadap aset kritis, penyebab potensial, penilaian tingkat risiko, dan mitigasi risiko terhadap aset kritis yang dimiliki oleh Dinas Pemberdayaan Perempuan, Perlindungan Anak dan Kependudukan Provinsi Jawa Timur.

3.1. Identifikasi Aset Kritis

Dinas Pemberdayaan Perempuan, Perlindungan Anak, dan Kependudukan didukung oleh akses kritis berupa hardware, software, network, data, dan people. Aset kritis ini digunakan untuk memenuhi kebutuhan dalam menjalankan aktivitas - aktivitas yang ada di dinas. Dan dengan adanya identifikasi aset kritis ini, dapat diketahui aset mana saja yang perlu diamankan dari setiap risiko yang ada. Adapun daftar aset yang dimiliki oleh dinas dapat dilihat dalam tabel 5.

Tabel 5. Identifikasi aset kritis

Kategori Aset	Aset Kritis
Hardware	Router Mikrotik
	Server
	Komputer

Kategori Aset	Aset Kritis
	Printer
	CCTV
Software	Aplikasi Super Sinden
	Aplikasi e-KembangPernik
	Aplikasi Siak Terpusat
Network	Perangkat Jaringan
Data	Data Administrasi Kependudukan Prov Jawa Timur
	Data Perencanaan Responsive Gender
People	Administrator data kependudukan
	Pengelola teknologi informasi

Berdasarkan tabel 5, dapat diketahui bahwa dinas setidaknya memiliki 13 aset yang dikelompokkan ke dalam 5 jenis yaitu hardware, software, network, data, dan people. Yang dimana dari ke 13 data tersebut akan diolah untuk mengetahui ancaman dan kerentanan terhadap setiap aset yang dimiliki dinas.

3.2. Ancaman dan Kerentanan pada aset kritis

Dari aset kritis yang telah dikelompokkan pada tabel 5, selanjutnya yaitu mengidentifikasi ancaman dan kerentanan apa saja yang dapat terjadi pada aset kritis tersebut. Ancaman dan kerentanan ini nanti yang dapat digunakan untuk menentukan risiko yang dapat dihadapi oleh setiap aset yang ada [7]. Data ancaman dan kerentanan terhadap setiap aset kritis yang ada dapat dilihat dalam tabel 6.

Tabel 6. Ancaman dan Kerentanan Aset Kritis

Aset Kritis	Kerentanan	Ancaman
Router Mikrotik	Ketahanan routing pada manajemen jaringan yang kurang memadai	Jaringan LAN lemot
Server	Server mengalami beban kerja yang tinggi	Server lambat
Komputer	Tidak menggunakan password yang kuat	Diakses oleh pihak yang tidak berwenang
Printer	Kurangnya pemeliharaan secara rutin	Rusaknya aset
CCTV	Terkena petir, atau bencana alam lain	CCTV rusak
Aplikasi Super Sinden	Karyawan kurang teliti dan kompeten	Aplikasi error
Aplikasi e-KembangPernik	Kurang perhatian akan pentingnya anti-virus	Aplikasi terserang virus
Aplikasi Siak terpusat	Kelemahan dalam mekanisme pengenalan dan autentikasi pengguna aplikasi.	Aplikasi mengalami serangan dari peretas atau terjadi upaya phising
Perangkat Jaringan	Manajemen jaringan rendah	Koneksi terputus atau menurun
Data Administrasi Kependudukan Prov Jawa Timur	Terlalu banyak data yang diinput	Database penuh
Data Perencanaan Responsive Gender	Kurangnya Backup data	Data mengalami kerusakan atau hilang
Administrator data kependudukan	Kurangnya pelatihan	Karyawan kurang teliti
Pengelola teknologi informasi	Kurangnya pelatihan	Tidak dapat menangani isu dengan efektif dan secara waktu yang singkat

3.3. Penyebab Potensial

Dari data ancaman dan kelemahan yang sudah teridentifikasi, selanjutnya dilakukan identifikasi penyebab potensial dan risiko pada setiap aset. Penyebab potensial merujuk pada kemungkinan terjadinya kegagalan atau dapat dikatakan sebagai faktor-faktor yang menyebabkan risiko terjadi [8]. Hasil identifikasi penyebab potensial selanjutnya dianalisis risiko yang mungkin terjadi berdasarkan penyebab potensial yang telah teridentifikasi. Tabel 7 merupakan data dari penyebab potensial dan risiko terhadap aset.

Tabel 7. Identifikasi Penyebab Potensial dan Risiko

Aset Kritis	Penyebab Potensial	Risiko
Router Mikrotik	Kurangnya mekanisme pemantauan terhadap jaringan	Hardware failure
Server	Spesifikasi server yang tidak memenuhi kebutuhan organisasi	Hardware failure
Komputer	Tidak logout saat meninggalkan komputer	Penyalahgunaan hak akses
Printer	Maintenance yang kurang teratur	Hardware failure
CCTV	Kerusakan fisik aset	Hardware failure
Aplikasi Super Sinden	Terjadi kesalahan dalam pemrograman fungsionalitas perangkat lunak	Software failure
Aplikasi e-KembangPernik	Komputer terserang virus	Hardware failure
Aplikasi Siak terpusat	Tidak ada perubahan yang dilakukan pada password secara reguler	Penyalahgunaan hak akses
Perangkat Jaringan	Gangguan jaringan pada provider	Network failure
Data Administrasi Kependudukan Prov Jawa Timur	Server down	Backup data failure
Data Perencanaan Responsive Gender	Kurang melakukan prosedur backup	Backup data failure
Administrator data kependudukan	Kesalahan penginputan data	Kehilangan atau tidak validnya data
Pengelola teknologi informasi	Kesalahan penggunaan sistem	Human atau technician error

3.4. Penilaian Tingkat Risiko Aset Kritis

Dari data identifikasi *potential cause* dan risiko pada setiap aset, dapat digunakan untuk melakukan penilaian tingkat risiko pada setiap aset. Penilaian tingkat risiko ini dapat digunakan untuk mengetahui level risiko setiap aset yang ada. Penilaian risiko atau yang disebut RPN, dapat diukur dengan menentukan nilai severity (S) atau tingkat keparahan dikali dengan nilai Occurrence (O) atau Keterjadian dikali dengan nilai Detection (D), untuk mendapatkan nilai risiko dari setiap aset yang ada. Level dalam RPN terdiri dari 5 kategori yaitu *very low* dengan nilai RPN < 51, *low* dengan nilai RPN < 101, *medium* dengan nilai RPN < 151, *high* dengan nilai RPN < 201, dan *very high* dengan nilai RPN > 200. Tabel 8 merupakan daftar penilaian risiko dari setiap aset yang dimiliki dinas.

Tabel 8. Penilaian Tingkat Risiko

Aset Kritis	Penyebab Potensial	Risiko	S	O	D	RPN	Level
Router Mikrotik	Kurangnya mekanisme pemantauan terhadap jaringan	Hardware failure	6	4	4	96	Low

Aset Kritis	Penyebab Potensial	Risiko	S	O	D	RPN	Level
Server	Spesifikasi server yang tidak memenuhi kebutuhan organisasi	Hardware failure	8	3	5	120	Medium
Komputer	Tidak logout saat meninggalkan komputer	Penyalahgunaan hak akses	6	4	3	72	Low
Printer	Maintenance yang kurang teratur	Hardware failure	5	5	6	150	Medium
CCTV	Kerusakan fisik aset	Hardware failure	6	3	5	90	Low
Aplikasi Super Sinden	Terjadi kesalahan dalam pemrograman fungsionalitas perangkat lunak	Software failure	8	4	6	192	High
Aplikasi e-KembangPernik	Komputer terserang virus	Hardware failure	8	5	5	200	High
Aplikasi Siak terpusat	Tidak ada perubahan yang dilakukan pada password secara reguler	Penyalahgunaan hak akses	8	3	5	120	Medium
Perangkat Jaringan	Gangguan jaringan pada provider	Network failure	5	4	6	120	Medium
Data Administrasi Kependudukan Prov Jawa Timur	Server down	Backup data failure	8	4	5	160	High
Data Perencanaan Responsive Gender	Kurang melakukan prosedur backup	Backup data failure	7	5	3	105	Medium
Administrator data kependudukan	Kesalahan penginputan data	Kehilangan atau tidak validnya data	7	3	2	42	Very Low
Pengelola teknologi informasi	Kesalahan penggunaan sistem	Human atau technician error	8	3	3	72	Low

3.5. Mitigasi

Setelah dilakukannya identifikasi aset, ancaman, risiko yang dihadapi, selanjutnya yaitu melakukan mitigasi risiko. Mitigasi risiko ini dilakukan untuk menurunkan dan memperbaiki tingkat risiko yang tinggi terhadap aset-aset yang ada. Mitigasi risiko yang dapat diterapkan dapat dilihat dalam tabel 9.

Tabel 9. Mitigasi Risiko

Aset Kritis	Risiko	Level	Tindakan Mitigasi Risiko
Router Mikrotik	96	Low	Melakukan monitoring dan maintenance jaringan secara berkala
Server	120	Medium	Memenuhi sesuai kebutuhan perusahaan
Komputer	72	Low	Pemanfaatan aset hanya dapat dilakukan terbatas sesuai dengan kebutuhan
Printer	150	Medium	Menentukan masa aset, kapan waktu ganti baru
CCTV	90	Low	Mengganti dengan yang baru
Aplikasi Super Sinden	192	High	Monitoring kinerja software secara berkala
Aplikasi e-KembangPernik	200	High	Pemeliharaan dan control secara berkala, serta memasang antivirus
Aplikasi Siak terpusat	120	Medium	Meningkatkan tingkat keamanan dengan menerapkan prosedur pengelolaan keamanan aset informasi

Aset Kritis	Risiko	Level	Tindakan Mitigasi Risiko
Perangkat Jaringan	120	Medium	Melakukan tindakan kontrol jaringan dengan cara di monitoring
Data Administrasi Kependudukan Prov Jawa Timur	160	High	Melakukan backup data secara berkala
Data Perencanaan Responsive Gender	105	Medium	Menerapkan pengendalian untuk memastikan integritas data dalam proses pencadangan
Administrator data kependudukan	42	Very Low	Menerapkan pengendalian dalam pengelolaan data, seperti prosedur verifikasi data yang diinput oleh staf yang bertanggung jawab sebagai administrator sistem
Pengelola teknologi informasi	72	Low	Diadakannya pelatihan keamanan sistem informasi secara rutin pada karyawan

Berdasarkan data yang didapatkan dapat diketahui bahwa terdapat 3 aset yang memiliki nilai risiko yang tinggi, 5 aset dengan nilai risiko medium, 4 aset dengan nilai risiko rendah, dan 1 aset dengan nilai risiko sangat rendah. Aset yang memiliki nilai risiko sangat rendah, rendah dan medium dapat dilakukan beberapa tindakan mitigasi yaitu berupa *monitoring*, *maintenance* aset secara berkala, pemanfaatan aset hanya dapat dilakukan terbatas sesuai dengan kebutuhan, dan perlu adanya pelatihan secara berkala untuk setiap karyawan.

Sedangkan untuk aset yang memiliki nilai risiko tinggi seperti aplikasi e-KembangPernik dengan nilai 200, yang memiliki kerentanan berupa kurangnya perhatian akan pentingnya anti virus menyebabkan ancaman berupa aplikasi yang terserang virus. Serta aplikasi ini memiliki penyebab potensial berupa PC yang terserang virus akibat aplikasinya yang terserang virus, menimbulkan risiko berupa *hardware failure*. Dari hal tersebut maka dapat dilakukan tindakan mitigasi risiko untuk mengurangi ataupun mencegah terjadinya risiko tersebut yaitu dengan melakukan pemeliharaan dan pengawasan secara berkala, serta memasang antivirus.

Untuk aset dengan nilai risiko tinggi kedua yaitu aplikasi Super Sinden dengan nilai 192, yang memiliki kerentanan berupa karyawan yang kurang teliti dan kompeten, sehingga menimbulkan ancaman berupa aplikasi error. Serta memiliki penyebab potensial berupa kesalahan koding pada fungsional software yang menimbulkan risiko berupa software *failure*. Dari hal tersebut maka dapat dilakukan tindakan mitigasi risiko berupa pemantauan kinerja software secara berkala agar dapat menurunkan tingkat risiko error terhadap software tersebut.

Untuk aset dengan nilai risiko tinggi yang terakhir yaitu berupa data administrasi kependudukan provinsi Jawa Timur dengan nilai 160, yang memiliki kerentanan berupa terlalu banyak data yang diinput, sehingga menyebabkan database penuh. Serta aplikasi ini juga memiliki penyebab potensial berupa *server down*, yang akan munculnya risiko berupa *backup data failure*. Dari hal tersebut maka dapat dilakukan tindakan mitigasi risiko agar dapat mengurangi adanya peningkatan risiko dengan melakukan backup data secara berkala.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah disampaikan, dapat diketahui bahwa Dinas Pemberdayaan Perempuan, Perlindungan Anak, dan Kependudukan Provinsi Jawa Timur memiliki banyak aset penting yang perlu dikelola keamanannya. Dari penelitian menggunakan metode OCTAVE diketahui setidaknya ada 13 aset penting yang dimiliki oleh dinas terkait. Ke 13 aset tersebut dikelompokkan menjadi 5 kategori yaitu hardware, software, data, network dan people. Setiap asetnya memiliki kerentanan dan risiko keamanan sistem informasi dalam penggunaannya. Berdasarkan hasil metode FMEA, dari 13 aset yang diteliti terdapat 3 aset yang memiliki nilai risiko yang tinggi, 5 aset dengan nilai risiko normal atau medium, 4 aset dengan nilai risiko rendah, dan 1 aset yang memiliki nilai risiko sangat rendah. Adapun aset dan risikonya yang memiliki nilai risiko tinggi yaitu aset aplikasi e-KembangPernik yang memiliki risiko

berupa *hardware failure*, aset aplikasi Super Sinden yang memiliki risiko berupa *software failure*, dan aset data administrasi kependudukan provinsi Jawa Timur yang memiliki risiko berupa *backup data failure*. Dan dari risiko tersebut dapat dilakukan tindakan mitigasi risiko untuk mengurangi atau mencegah terjadinya peningkatan nilai risiko. Tindakan mitigasi risiko tersebut dapat berupa melakukan pemeliharaan dan pengawasan secara berkala, serta memasang antivirus, monitoring kinerja software, dan melakukan backup data secara berkala.

5. SARAN

Saran yang dapat diberikan pada penelitian selanjutnya yaitu peneliti dapat mengajukan kuesioner kepada masing-masing anggota divisi untuk mendapatkan data aset secara rinci dan risiko - risiko yang ada pada setiap aset agar dapat meminimalisir terjadinya risiko tersebut, diharapkan juga para peneliti selanjutnya mampu menurunkan jumlah risiko dan nilai risiko pada setiap aset. Serta peneliti selanjutnya dapat menentukan mitigasi risiko yang lebih efektif lagi untuk menurunkan tingkat risiko yang ada.

DAFTAR PUSTAKA

[1] Christina, D. D., Rochim, A. I., & Kusbandrijo, B., 2022. Implementasi Kebijakan Peraturan Gubernur Jawa Timur Nomor 1 Tahun 2021 Bab IV tentang Uraian Tugas dan Fungsi: (Studi Kasus di UPT PPA Jawa Timur Kota Surabaya). PRAJA observer: Jurnal Penelitian Administrasi Publik (e-ISSN: 2797-0469), 2(05), 61-69.

[2] Budiarto, R., 2017. Penerapan Metode FMEA Untuk Keamanan Sistem Informasi (Studi Kasus: Website POLRI). In: Prosiding 2nd Seminar Nasional IPTEK Terapan (SENIT) (Vol. 2, No. 1, pp. 73-78).

[3] Dianta, I. A., & Zusrony, E., 2019. Analisis Pengaruh Sistem Keamanan Informasi Perbankan Pada Nasabah Pengguna Internet Banking. INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi, 3(1), 1-9.

[4] Nelmiawati, N., Destrianto, F. R., & Sitorus, M. A. R., 2017. Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE. Jurnal Integrasi, 9(1), 35-47.

[5] Hisprastin, Y., & Musfiroh, I., 2021. Ishikawa diagram dan failure mode effect analysis (FMEA) sebagai metode yang sering digunakan dalam manajemen risiko mutu di industri. Majalah Farmasetika, 6(1), 1-9.

[6] Putri, P. N., & Hadi, H. P., 2017. Analisis Evaluasi Dan Mitigasi Risiko Aset Teknologi Informasi Menggunakan Framework OCTAVE dan FMEA Pada Bank Jateng Cabang Jepara. JOINS (Journal of Information System), 2(2), 213-226.

[7] Nafasari, A., & Sari, W. S., 2018. Analisis dan Mitigasi Risiko Aset Kritis Terhadap Kegagalan Proses Produksi Penyiaran Di TVKU Semarang Menggunakan Metode OCTAVE Dan FMEA. JOINS (Journal of Information System), 3(2), 171-179.

[8] Pakarbudi, A., Piay, D. T., Nurmadewi, D., & Rachman, A., 2023. Analisa Efektivitas Metode Octave Allegro dan Fmea Dalam Penilaian Risiko Aset Informasi Pada Institusi Pendidikan Tinggi. JURIKOM (Jurnal Riset Komputer), 10(2), 488-496.