Analisis Risiko Keamanan Sistem Informasi Website Rekrutmen Fast Print Indonesia menggunakan Metode OCTAVE dan FMEA

Fadiyah Dhara Al Arsya*[1], Eristya Maya Safitri[2], Dinda Adisty Yudianto Putri[3], Efriza Cahya Narendra[4]
Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur
e-mail: [1]fadiyaharsya@gmail.com, [2]maya.si@upnjatim.ac.id, [3]dndadisty@gmail.com, [4]efrizac03@gmail.com
*Penulis Korespodensi

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

Abstrak

Seiring berkembangnya teknologi, banyak instansi yang memanfaatkannya untuk mendukung operasional bisnis, termasuk CV Fast Print Indonesia. Instansi ini mengembangkan website rekrutmen untuk mengelola data dan informasi. Namun terdapat permasalahan pada keamanan data yang dapat menyebabkan kerugian, sehingga penelitian ini diharapkan dapat melakukan identifikasi ancaman, menganalisis risiko dan penanganan risiko terhadap aset yang dimiliki. Metode penelitian yang digunakan adalah metode OCTAVE dan FMEA. Hasil penelitian menunjukkan bahwa terdapat 11 aset penting pada CV Fast Print Indonesia yang terbagi menjadi 5 golongan yakni, hardware, software, network, people, dan data. Dari aset tersebut terdapat 3 aset yang memiliki risiko very high, 1 aset yang memiliki risiko high, 2 aset yang memiliki risiko medium, 3 aset yang memiliki risiko low dan 2 aset yang memiliki risiko very low. Sehingga CV Fast Print perlu mengelola keamanan informasi dengan baik untuk melindungi aset yang dimiliki. Penelitian ini juga membuktikan bahwa penggunaan metode OCTAVE dan FMEA sangat efektif untuk menentukan keamanan sistem informasi pada CV Fast Print Indonesia. Oleh karena itu, kedua metode ini dapat dijadikan solusi untuk melakukan analisis keamanan sistem informasi agar dapat membantu instansi dalam melakukan manajemen keamanan sistem informasi.

Kata kunci: *Keamanan Sistem Informasi, OCTAVE, FMEA, Analisis Risiko, Website Recruitment*

Abstract

As technology develops, many agencies use it to support business operations, including CV Fast Print Indonesia. This agency develops a recruitment website to manage data and information. However, there are problems with data security that can cause losses, so this research is expected to be able to identify threats, analyze risks and handle risks to assets owned. The research method used is the OCTAVE and FMEA methods. The results of the study show that there are 11 important assets in CV Fast Print Indonesia which are divided into 5 groups namely, hardware, software, network, people, and data. Of these assets, there are 3 assets with very high risk, 1 asset with high risk, 2 assets with medium risk, 3 assets with low risk and 2 assets with very low risk. So that CV Fast Print needs to manage information security properly to protect its assets. This study also proves that the use of the OCTAVE and FMEA methods is very effective for determining information system security at CV Fast Print Indonesia. Therefore, these two methods can be

used as a solution for conducting information system security analysis in order to assist agencies in conducting information system security management.

***Keywords**: Information security, OCTAVE, FMEA, Risk analysis, Website Recruitment*

1. PENDAHULUAN

Seiring berkembangnya zaman, teknologi telah menjadi kebutuhan utama bagi hampir semua aspek kehidupan. Saat ini, teknologi informasi banyak dimanfaatkan instansi untuk keperluan bisnisnya [1]. Salah satu instansi yang memanfaatkan teknologi adalah CV Fast Print Indonesia. CV Fast Print Indonesia merupakan perusahaan yang menyediakan bahan baku percetakan. Perusahaan ini telah mengembangkan website rekrutmen yang bertujuan untuk memudahkan proses penerimaan tenaga kerja baru serta penyebaran informasi mengenai lowongan kerja. Website ini menyediakan informasi mengenai posisi yang tersedia, persyaratan yang dibutuhkan serta prosedur untuk mengajukan lamaran. Calon pelamar dapat mengunggah berkas yang dibutuhkan seperti CV dan data pribadi. Tim rekrutmen dapat melihat berkas unggahan calon pelamar untuk bahan pertimbangan penerimaan calon pelamar.

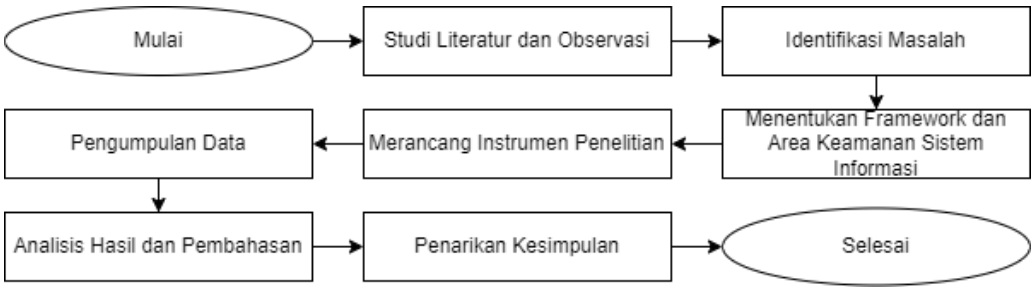
Namun pada website ini memiliki beberapa permasalahan, seperti keamanan data. Calon pelamar khawatir terkait keamanan dan privasi data mereka. Sehingga pelanggaran privasi dan keamanan data merupakan hal yang perlu diwaspadai agar calon pelamar tidak perlu khawatir dan dapat mengajukan lamaran dengan tenang. Untuk mengatasi permasalahan tersebut, CV Fast Print Indonesia dapat meningkatkan dan melakukan pemeliharaan sistem dengan baik untuk dapat meminimalisir kesalahan yang terjadi. Sehingga, penting untuk memiliki keamanan sistem yang kokoh untuk memastikan keamanan data dan informasi.

Berdasarkan permasalahan tersebut, terdapat metode OCTAVE dan FMEA yang dapat digunakan untuk menganalisis manajemen risiko pada CV Fast Print Indonesia. Metode OCTAVE dapat membantu menganalisis ancaman dan kerentanan pada sistem. Metode FMEA membantu untuk menganalisis kegagalan serta dampak dari kegagalan tersebut sehingga dapat menemukan solusi yang tepat untuk mengatasi permasalahan pada website recruitment CV Fast Print Indonesia.

Oleh sebab itu, penelitian ini diharapkan dapat membantu CV Fast Print Indonesia terkait manajemen keamanan sistem informasi pada website rekrutmen. Sehingga CV Fast Print Indonesia dapat meningkatkan keamanan sistem informasi pada website *rekrutmen* tersebut. Hal ini untuk memastikan bahwa CV Fast Print Indonesia dapat melindungi data keamanan dengan baik.

2. METODE PENELITIAN

Pada metode penelitian ini akan menjelaskan secara detail tentang metode yang digunakan.



Gambar 1. Metode Penelitian

Pada metode penelitian ini terdapat beberapa tahapan, yakni studi literatur dan observasi, identifikasi masalah, menentukan framework dan area keamanan sistem informasi, merancang instrumen penelitian, pengumpulan data, analisis hasil dan pembahasan serta penarikan kesimpulan. Metode penelitian terdapat pada gambar 1.

2.1. Studi Literatur dan Observasi

Studi literatur bertujuan untuk memperoleh informasi mengenai manajemen keamanan risiko sistem informasi. Studi literatur ini dapat diperoleh melalui beberapa sumber, seperti jurnal, buku dan lain sebagainya. Data yang didapatkan akan digunakan untuk menganalisis manajemen risiko keamanan sistem informasi.

Observasi berupa wawancara bertujuan untuk memperoleh data dan informasi lebih rinci mengenai CV Fast Print Indonesia. Wawancara dilakukan dengan senior programmer CV Fast Print Indonesia [2]. Hasil data dan informasi yang diperoleh dari wawancara akan digunakan untuk menganalisis keamanan sistem informasi pada CV Fast Print Indonesia.

2.2. Identifikasi Masalah

Pada identifikasi masalah berisi mengenai permasalahan terkait topik dari penelitian ini. Masalah yang diambil dalam penelitian ini adalah mengenai manajemen risiko keamanan sistem informasi pada website rekrutmen CV Fast Print Indonesia. Pemilihan permasalahan tersebut dikarenakan pada website rekrutmen CV Fast Print Indonesia ini menyimpan data pribadi calon pelamar sehingga calon pelamar khawatir akan keamanan datanya. Oleh karena itu, instansi ini perlu menerapkan manajemen risiko keamanan sistem informasi yang baik.

2.3. Menentukan Framework dan Area Keamanan Sistem Informasi

Metode OCTAVE digunakan dalam pengelolaan data yang didapatkan melalui proses wawancara. Metode ini bertujuan untuk melakukan analisis terkait risiko pada keamanan sistem informasi. Terdapat tiga tahapan metode OCTAVE. Tahapan pertama yaitu menyusun ancaman berdasarkan aset data yang dimiliki oleh CV Fast Print Indonesia. Tahapan kedua yaitu melakukan identifikasi kerentanan infrastruktur yang ada pada CV Fast Print Indonesia. Tahapan ketiga yaitu proses evaluasi dengan melakukan identifikasi terhadap aset yang berpotensi menimbulkan bahaya. Selanjutnya melakukan penanganan dengan merancang rencana yang spesifik.

Metode FMEA digunakan untuk melakukan identifikasi serta menentukan prioritas kegagalan agar dapat melakukan pencegahan. Selain itu, juga digunakan untuk memberikan penilaian risiko aset kritis menggunakan data yang telah didapatkan dari hasil analisis menggunakan metode OCTAVE [3]. Terdapat empat tahapan dalam metode FMEA, meliputi Severity (S), Occurrence (O), Detection (D), dan Risk Priority Number (RPN). Severity (S) merupakan tingkat keparahan yang berupa penilaian terhadap potensi tertinggi kegagalan. Skala tingkat keparahan dapat dilihat dalam tabel 1. Occurrence (O) atau kejadian merupakan skala waktu terjadinya kegagalan pada setiap aset. Skala tingkat kejadian dapat dilihat dalam tabel 2. Detection (D) atau deteksi merupakan evaluasi terhadap kemungkinan teridentifikasinya penyebab kegagalan. Skala deteksi terdapat dalam tabel 3. Risk Priority Number (RPN) merupakan hasil perkalian Severity, Occurrence dan Detection dengan rumus RPN= S x O x D. Skala nilai RPN terdapat dalam tabel 4.

Tabel 1. Skala tingkat keparahan

Dampak	Kriteria	Peringkat
Berbahaya: Tanpa Peringkat	Pekerja dapat terjadi cedera	10
Berbahaya: Tanpa Peringkat	Tindakan yang melanggar kebijakan perusahaan	9

Dampak	Kriteria	Peringkat
Sangat Tinggi	Terdapat kesalahan dalam penggunaan peralatan yang tersedia	8
Tinggi	Customer akan komplain	7
Sedang	Kerugian dapat terjadi untuk perusahaan	6
Rendah	Pekerja menjadi menurun untuk kinerjanya	5
Sangat Rendah	Terjadi sedikit kerugian	4
Minor	Terdapat gangguan kecil tanpa adanya kehilangan	3
Sangat Minor	Terdapat dapat kecil kepada kinerja dan terjadi tanpa disadari	2
Tidak berdampak	Tidak ada pengaruh kinerja dan terjadi tanpa disadari	1

Tabel 2. Skala tingkat kejadian

Probabilitas Risiko	Periode Waktu	Peringkat
Sangat Tinggi	Lebih dari sekali setiap hari	10
Tinggi : tingkat kegagalan yang tidak dapat dihindari	Sekali setiap 4 hari	9
Tinggi : terkait dengan proses yang sering mengalami kegagalan sebelumnya	Sekali setiap minggu	8
Sering terjadi kegagalan	Sekali setiap bulan	7
Moderate : sebelumnya sering mengalami kegagalan	Sekali setiap 3 bulan	6
Proses sebelumnya yang jarang mengalami kegagalan	Sekali setiap 6 bulan	5
Kegagalan yang terjadi sebelumnya, tetapi dalam proporsi yang kecil	Sekali setiap setahun	4
Rendah : terjadi kegagalan dengan proses yang sejenis	Sekali setiap 1-3 tahun	3
Sangat Rendah : kegagalan terjadi namun hanya pada proses yang identik	Sekali setiap 3-6 tahun	2
Remote : tidak akan terjadi kegagalan	Sekali setiap 6-100 tahun	1

Tabel 3. Skala deteksi

Deteksi	Kriteria	Peringkat
Sangat sulit terjadi	Pengendalian tidak mampu mendeteksi kegagalan	1
Sangat kecil	Potensi kegagalan sangat jauh untuk ditemukan	2
Kecil	Potensi kegagalan jarang ditemukan	3
Tingkatannya sangat rendah	Potensi sangat rendah untuk menemukan kegagalan	4
Tingkatannya rendah	Potensi rendah untuk menemukan kegagalan	5
Tingkatannya sedang	Potensi sedang untuk menemukan kegagalan	6
Tingkatannya cukup tinggi	Potensi cukup tinggi untuk menemukan kegagalan	7
Tingkatannya tinggi	Potensi tinggi untuk menemukan kegagalan	8
Tingkatannya sangat tinggi	Potensi sangat tinggi untuk menemukan kegagalan	9
Hampir pasti terjadi	Kegagalan dalam proses tidak mungkin terjadi karena telah diantisipasi melalui sistem solusi	10

Tabel 4. Nilai RPN

Level Risiko	RPN
Very High	200 >
High	151 - 200
Medium	101 - 150
Low	51 - 100
Very Low	0 - 50

2.4. Merancang Instrumen Penelitian

Pada tahap ini merupakan tahapan untuk melakukan rancangan instrumen penelitian. Merancang instrumen penelitian dengan melakukan pengumpulan data melalui wawancara yang

dilakukan dengan senior programmer pada CV Fast Print Indonesia. Metode OCTAVE dapat digunakan sebagai acuan dalam melakukan wawancara. Hal ini dapat membantu peneliti untuk mengumpulkan data yang digunakan untuk penelitian ini. Selain itu, dengan melakukan wawancara juga bertujuan agar dapat mengetahui aset apa saja yang dimiliki CV Fast Print Indonesia, gangguan dan risiko yang pernah terjadi pada instansi serta hal yang dilakukan oleh CV Fast Print Indonesia untuk melakukan penanganan pada risiko yang terjadi tersebut.

2.5. Pengumpulan Data

Data kualitatif adalah data yang didapatkan mengenai permasalahan dari objek penelitian. Pada penelitian ini, sumber data informasi diperoleh dari wawancara yang telah dilakukan dengan senior programmer pada CV Fast Print Indonesia. Pada data kualitatif ini mengacu pada penggunaan metode OCTAVE yang digunakan untuk menganalisis aset yang dimiliki oleh CV Fast Print Indonesia.

Data kuantitatif merupakan data yang didapatkan secara sistematis. Pada penelitian ini, data didapatkan berdasarkan penerapan metode FMEA. Dengan metode ini, bertujuan untuk melakukan penilaian terhadap risiko aset dengan menghasilkan nilai RPN [4].

2.6. Analisis Hasil dan Pembahasan

Pada analisis hasil dan pembahasan ini merupakan proses analisis data yang telah dikumpulkan. Dengan metode OCTAVE dan FMEA dapat dilakukan analisis data. Setelah melakukan analisis data menggunakan kedua metode tersebut, hasilnya dapat digunakan untuk CV Fast Print Indonesia dalam melakukan manajemen keamanan sistem informasi.

2.7. Penarikan Kesimpulan

Pada penarikan kesimpulan ini merupakan tahapan yang digunakan untuk menarik kesimpulan dari hasil analisis data yang telah dilakukan. Pada kesimpulan ini berisi ringkasan dari penelitian yang berisi data dan informasi.

3. HASIL DAN PEMBAHASAN

Bab ini membahas tentang identifikasi aset kritis, keperluan kebutuhan keamanan, identifikasi ancaman dan kerentanan aset informasi, identifikasi penyebab potensial, penilaian risiko, mitigasi risiko yang ada pada CV Fast Print Indonesia.

3.1. Identifikasi Aset Kritis

Wawancara telah dilakukan dengan senior programmer pada CV Fast Print Indonesia. Dengan wawancara tersebut, peneliti dapat melakukan pengumpulan data yang dibutuhkan. Data yang telah dikumpulkan dapat mengidentifikasi kategori aset. Hasil dari identifikasi akan ditampilkan pada tabel 5.

Tabel 5. Identifikasi aset kritis

Kelompok Aset	Aset Kritis
Hardware	Komputer (CPU, Monitor) Switch Server
Software	OS/Operating System (Windows) Sistem informasi website Antivirus
Network	Router

Kelompok Aset	Aset Kritis
	Modem internet
Pengguna/People	Admin website rekrutmen
Data	Data pelamar
	Data informasi

3.2. Penggunaan Gambar

Setelah melakukan proses identifikasi aset yaitu mengidentifikasi kebutuhan keamanan untuk setiap aset yang ada. Aset-aset tersebut diidentifikasi dengan mempertimbangkan aspek *confidentiality* (kerahasiaan), *integrity* (keutuhan), dan *availability* (ketersediaan). Identifikasi kebutuhan keamanan ini bertujuan untuk menjaga kelangsungan bisnis dan meminimalisir risiko. Hasil dari identifikasi kebutuhan keamanan terdapat pada tabel 6.

Tabel 6. Kebutuhan keamanan

Aset Kritis	Kebutuhan Keamanan		
	Confidentiality	Integrity	Availability
Hardware: Komputer, Switch, Server	Akses hanya tersedia untuk admin dan atasan	Hanya boleh diakses oleh pihak yang bersangkutan	Akses hardware harus tersedia selalu
Software: OS, Sistem informasi website, Anti virus	Hanya pihak yang memiliki wewenang yang boleh mengakses aplikasi	Informasi harus lengkap dan akurat	Melakukan update secara berkala
Network: Router, Modem internet	Memastikan tidak ada pelanggaran yang dapat menimbulkan masalah	Memastikan keaslian data	Selalu memantau peralatan untuk jaringan.
People: Admin website recruitment	Memastikan menjaga keamanan data dari pihak yang tidak berwenang	Memastikan keakuratan data dan informasi	Admin sistem informasi harus sering mengupdate sistem yang ada.
Data: Pelamar, Informasi	Hanya dapat diakses oleh pihak yang bersangkutan	Data harus lengkap dan akurat	Data yang bisa selalu diakses

3.3. Identifikasi Ancaman dan Kerentanan Aset Informasi

Setelah mengidentifikasi kebutuhan keamanan selanjutnya melakukan identifikasi terhadap kerentanan dan ancaman yang terdapat pada setiap aset. Tujuan dari identifikasi kerentanan adalah untuk menentukan aset yang rentan terhadap potensi bahaya. Identifikasi ancaman dilakukan untuk mengetahui faktor yang dapat mengancam aset tersebut [5]. Hasil identifikasi kerentanan dan ancaman terdapat pada tabel 7.

Tabel 7. Kebutuhan keamanan

Aset Kritis	Kerentanan	Ancaman
Komputer (CPU, Monitor)	Kerentanan terhadap voltase yang bervariasi	Hilangnya pasokan listrik
Switch	Serangan Denial-of-Service (DoS)	Penurunan kinerja jaringan atau bahkan kegagalan total
Server	Beban kerja server yang tinggi	AC di ruangan server mati/rusak
OS/Operating System (Windows)	Terserang malware	kerusakan sistem, mencuri informasi sensitif, atau mengganggu kinerja sistem operasi
Sistem informasi website	Mekanisme otentikasi pada aplikasi masih kurang	Aplikasi terserang hacker

Aset Kritis	Kerentanan	Ancaman
Antivirus	Terjadinya phising	Penyerang dapat memasukkan malware atau mendapatkan akses ke sistem pengguna
Router	Ketahanan jaringan masih kurang	Jaringan LAN lemot
Modem internet	Peletakan kabel sembarangan	Gangguan dalam akses internet dan menyebabkan ketidaknyamanan atau kerugian bagi pengguna
Admin website recruitment	Kurangnya mekanisme pemantauan	Karyawan kurang teliti
Data pelamar	Data yang diinput terlalu banyak	Database penuh
Data informasi	Pengupdatean terlalu sering dilakukan	Redudansi Data

3.4. Identifikasi Penyebab Potensial

Setelah mengidentifikasi kerentanan dan ancaman yaitu mengidentifikasi penyebab potensial. Identifikasi penyebab potensial ini bertujuan agar dapat mengetahui faktor yang dapat menyebabkan kegagalan terjadi. Hasil identifikasi dapat dianalisis untuk mengevaluasi risiko yang mungkin terjadi. Rincian penyebab potensial dan analisis risiko terdapat pada tabel 8.

Tabel 8. Penyebab potensial

Aset Kritis	Penyebab Potensial	Risiko
Komputer (CPU, Monitor)	Korsleting listrik	Kebakaran
Switch	Kerentanan keamanan switch	Gangguan jaringan
Server	Server overheat	Hardware failure
OS/Operating System (Windows)	Serangan exploit OS	Kehilangan data
Sistem informasi website	Password tidak pernah diganti	Penyalahgunaan hak akses
Antivirus	Ketidakterdeteksian malware	Kehilangan data
Router	Serangan firewall bypass	Penetrasi jaringan
Modem internet	Serangan phising	Pencurian data pribadi
Admin website recruitment	Kurangnya mekanisme pemantauan	Karyawan kurang teliti
Data pelamar	Kehilangan atau pencurian data	Pelanggaran privasi
Data informasi	Akses tidak sah ke informasi pengguna	Penyalahgunaan data

3.5. Penilaian Risiko

Setelah mengidentifikasi penyebab potensial selanjutnya melakukan penilaian risiko. Risiko dapat disebabkan oleh beberapa faktor. Dengan melakukan perhitungan Risk Priority Number (RPN) dapat menemukan hasil penilaian risiko. Hasil penilaian tersebut ditampilkan pada tabel 9.

Tabel 9. Hasil penilaian resiko

Aset Data	Penyebab Potensial	Risiko	SEV	OCC	DEC	RPN	Level
Komputer (CPU, Monitor)	Korsleting listrik	Kebakaran	5	1	10	50	Very Low
Switch	Kerentanan keamanan switch	Gangguan jaringan	5	8	6	240	Very High
Server	Server overheat	Hardware failure	7	5	8	280	Very High
OS/Operating System (Windows)	Serangan exploit OS	Kehilangan data	5	4	4	80	Low

Aset Data	Penyebab Potensial	Risiko	SEV	OCC	DEC	RPN	Level
Sistem informasi website	Tidak pernah mengganti password	Hak akses yang disalahgunakan	7	3	6	126	Medium
Antivirus	ketidakterdeteksian malware	Penyebaran malware, kehilangan data	5	1	7	35	Very Low
Router	Serangan firewall bypass	Penetrasi jaringan	5	5	7	175	High
Modem internet	Serangan phising	Pencurian data pribadi	5	5	5	125	Medium
Admin website rekrutmen	Kurangnya mekanisme pemantauan	Karyawan kurang teliti	7	8	4	224	Very High
Data pelamar	Kehilangan atau pencurian data	Pelanggaran privasi	9	1	7	63	Low

3.6. Mitigasi Risiko

Setelah melakukan penilaian risiko selanjutnya melakukan mitigasi risiko. Mitigasi risiko dilakukan melalui wawancara dengan pihak yang bertanggung jawab terkait website rekrutmen pada CV Fast Print Indonesia. Hasil dari mitigasi risiko terdapat pada tabel 10.

Tabel 10. Mitigasi risiko

Aset Data	Risiko	Level	Tindakan mitigasi risiko
Komputer (CPU, Monitor)	Kebakaran	Very Low	Melakukan perlindungan terhadap aset teknologi yang dimiliki.
Switch	Gangguan jaringan	Very High	Mengaktifkan fitur keamanan seperti VLAN dan Port Security untuk mencegah akses tidak sah ke switch.
Server	Hardware failure	Very High	Melakukan pemantauan secara berkala agar dapat berjalan sesuai rencana
OS/Operating System (Windows)	Kehilangan data	Low	Memperbarui sistem operasi secara teratur untuk mengatasi kerentanan keamanan yang diketahui.
Sistem informasi website	Penyalahgunaan hak akses	Medium	Memperbarui sistem informasi website secara teratur untuk mengatasi kerentanan keamanan yang diketahui.
Antivirus	Penyebaran malware, kehilangan data	Very Low	Menginstal dan memperbarui perangkat lunak anti-virus yang terkemuka dan mengkonfigurasi pemindaian secara teratur.
Router	Penetrasi jaringan	High	Mengubah password default router dan menggunakan password yang kuat.
Modem internet	Pencurian data pribadi	Medium	Menggunakan teknik pengujian keamanan untuk mengidentifikasi kerentanan pada modem internet.
Admin website rekrutmen	Karyawan kurang teliti	Very High	Mengimplementasikan sistem logging dan monitoring yang memungkinkan pemantauan aktivitas admin yang mencurigakan.
Data pelamar	Pelanggaran privasi	Low	Mengimplementasikan kebijakan akses yang ketat untuk membatasi akses terhadap data pelamar.

Aset Data	Risiko	Level	Tindakan mitigasi risiko
Data informasi	Penyalahgunaan data	Low	Mengimplementasikan kebijakan akses yang ketat untuk membatasi akses terhadap data informasi.

3.7. Rekomendasi

Dari informasi yang diperoleh, dapat disimpulkan bahwa terdapat tiga aset dengan risiko yang sangat tinggi, satu aset dengan risiko tinggi, dua aset dengan risiko sedang, tiga aset dengan risiko rendah, dan dua aset dengan risiko sangat rendah. Untuk aset-aset dengan risiko sangat rendah, rendah, dan sedang, beberapa langkah mitigasi dapat dilakukan, seperti melakukan pemantauan secara teratur, pemeliharaan berkala terhadap aset, serta membatasi penggunaan aset sesuai dengan kebutuhan yang ada.

Sedangkan untuk aset yang memiliki nilai risiko *very high* seperti switch dengan nilai 240, yang memiliki kerentanan berupa serangan DoS menyebabkan ancaman berupa penurunan kinerja jaringan atau kegagalan total. Serta aplikasi ini memiliki penyebab potensial berupa kerentanan keamanan switch, menimbulkan risiko berupa gangguan jaringan. Dari hal tersebut maka dapat dilakukan tindakan mitigasi risiko berupa mengaktifkan fitur keamanan seperti VLAN dan port security untuk mencegah akses tidak sah ke switch.

Untuk aset dengan nilai risiko *very high* kedua yaitu server dengan nilai 280, yang memiliki kerentanan berupa beban kerja server yang tinggi, sehingga menimbulkan ancaman berupa ACs di ruangan server mati atau rusak. Serta memiliki penyebab potensial berupa server *overheat* yang menimbulkan risiko berupa *hardware failure*. Dari hal tersebut maka dapat dilakukan tindakan mitigasi risiko berupa melakukan pemantauan secara berkala agar dapat berjalan sesuai rencana.

Untuk aset dengan nilai risiko *high* yang terakhir yaitu admin website rekrutmen dengan nilai 224, yang memiliki kerentanan berupa kurangnya mekanisme pemantauan, sehingga menyebabkan ancaman yaitu karyawan yang kurang teliti. Serta aplikasi ini juga memiliki penyebab potensial berupa kurangnya mekanisme pemantauan, yang akan munculnya risiko berupa karyawan yang kurang teliti. Dari hal tersebut maka dapat dilakukan tindakan mitigasi risiko agar dapat mengurangi adanya peningkatan risiko dengan mengimplementasikan sistem log dan monitoring yang memungkinkan pemantauan aktivitas admin yang mencurigakan.

4. KESIMPULAN

Pada penelitian ini dapat disimpulkan bahwa yaitu CV Fast Print Indonesia memiliki 11 aset penting yang perlu dijaga keamanannya. Seluruh aset penting tersebut dapat diidentifikasi menggunakan metode OCTAVE. Aset penting tersebut dikelompokkan menjadi 5 kategori yakni, hardware, software, network, people, dan data. Dengan melakukan analisis manajemen risiko menggunakan OCTAVE, dapat membantu CV Fast Print Indonesia dalam pengelolaan manajemen keamanan sistem informasi. Selain itu, hasil analisis menggunakan metode FMEA memiliki 3 aset yang memiliki risiko *very high*, 1 aset yang memiliki risiko *high*, 2 aset yang memiliki risiko medium, 3 aset yang memiliki risiko *low* dan 2 aset yang memiliki risiko *very low*. Dari hasil tersebut menunjukkan bahwa terdapat beberapa data memiliki risiko tinggi sehingga perlu dilakukannya mitigasi risiko dari CV Fast Print Indonesia untuk mencegah atau mengurangi terjadinya ancaman risiko.

5. SARAN

Saran yang untuk penelitian selanjutnya adalah dengan melakukan analisis terhadap ancaman terbaru terhadap studi kasus tertentu. Sehingga pada penelitian selanjutnya dapat

menyesuaikan perkembangan ancaman terbaru. Hal itu diharapkan dapat menurunkan jumlah risiko pada setiap aset serta dapat menentukan mitigasi risiko yang efektif dan sesuai dengan studi kasus yang diambil.

DAFTAR PUSTAKA

[1] G. Setyadi dan Y. Kusumawati, "Mitigasi Risiko Aset dan Komponen Teknologi Informasi Berdasarkan Kerangka Kerja OCTAVE dan FMEA pada Universitas Dian Nuswantoro," Journal of Information System, pp. 1-10.

[2] A. H. Putri dan Y. Kusumawati, "Strategi Mitigasi Risiko Aset Kritis Teknologi Informasi Menggunakan Metode OCTAVE dan FMEA," Techno.COM, vol. 16, no. 4, pp. 367-377, 2017.

[3] A. Nafasari dan W. S. Sari, "Analisis dan Mitigasi Risiko Aset Kritis Terhadap Kegagalan Proses Produksi Penyiaran di TVKU Semarang Menggunakan Metode OCTAVE dan FMEA," Journal of Information System , vol. 3, no. 2, pp. 171-179, 2018.

[4] P. N. Putri dan H. P. Hadi, "Analisis, Evaluasi, dan Mitigasi Risiko Aset Teknologi Informasi Menggunakan Framework OCTAVE dan FMEA pada Bank Jateng Cabang Jepara," JOINS, vol. 2, no. 2, pp. 213-226, 2017.

[5] A. Pakarbudi, D. T. Piay, D. Nurmadewi dan A. Rachman, "Analisa Efektivitas Metode OCTAVE Allegro dan Fmea dalam Penilaian Risiko Aset Informasi pada Institusi Pendidikan Tinggi," Jurnal Riset Komputer, vol. 10, no. 2, pp. 488-496, 2023.