Neptunus : Jurnal Ilmu Komputer Dan Teknologi Informasi
Volume. 3, Nomor. 2, Mei 2025
e-ISSN : 3031-898X; dan p-ISSN : 3031-8998; Hal. 65-76
DOI: https://doi.org/10.61132/neptunus.v3i2.796
Available online at: https://journal.arteii.or.id/index.php/Neptunus

Analisis dan Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Metode OCTAVE dan FMEA Berbasis ISO 27001:2022
(Studi Kasus : Perusahaan XYZ)

Ajeng Wahyuningtyas[1*], Ni Made Ika Marini Mandenni[2], Muhammad Alam Pasirulloh[3]
[1,2,3] Universitas Udayana, Indonesia

Alamat: Jl. Raya Kampus Unud, Jimbaran, Kuta Selatan, Badung-Bali-80361
Korespondensi penulis: ningtyasajeng24@student.unud.ac.id

Abstract. *The advancement of information technology has driven companies to adopt technology-based systems to enhance operational efficiency while also increasing the complexity of information security risks. This study aims to analyse risk factors associated with information security assets, identify potential threats, assess risks, and provide mitigation recommendations. The OCTAVE method was applied to identify threats, vulnerabilities, and critical information technology assets, while FMEA was used to determine risk mitigation priorities based on the Risk Priority Number (RPN). The mitigation recommendations were developed in accordance with ISO 27001:2022 standards. Data collection was conducted through interviews with XYZ company representatives, identifying 34 information security asset risks, including 6 hardware failure potentials, 6 software failure potentials, 14 data failure potentials, 4 human resource failure potentials, and 4 network failure potentials. The risk categorisation results revealed 5 high-level risks, 6 moderate-level risks, 20 low-level risks, and 3 very low-level risks. The mitigation recommendations include three ISO/IEC 27001:2022 clauses: Human Resource Controls, Physical Controls, and Information Technology Controls.*

Keywords: *Information Technology, Information Security, Risk Management, OCTAVE, FMEA*

Abstrak. Kemajuan teknologi informasi mendorong perusahaan mengadopsi sistem berbasis teknologi untuk meningkatkan efisiensi operasional, namun juga memperumit risiko keamanan informasi. Penelitian ini bertujuan untuk menganalisis faktor risiko aset keamanan informasi, mengidentifikasi, menilai serta memberikan rekomendasi mitigasi. Metode OCTAVE digunakan untuk mengidentifikasi ancaman, kerentanan aset teknologi informasi kritis, sementara FMEA diterapkan untuk menentukan prioritas mitigasi risiko berdasarkan *Risk Priority Number* (RPN). Rekomendasi yang dihasilkan mengacu pada standar ISO 27001:2022. Pengumpulan data penelitian dilakukan melalui wawancara dengan pihak Perusahaan XYZ dengan memperoleh 34 risiko aset keamanan informasi dengan 6 potensi kegagalan pada perangkat keras, 6 potensi kegagalan pada perangkat lunak, 14 potensi kegagalan pada data, 4 potensi kegagalan pada sumber daya manusia, dan 4 potensi kegagalan pada jaringan. Hasil pengkategorian risiko tersebut didapatkan 5 risiko kategori tingkat tinggi (*high*), 6 risiko kategori tingkat sedang (*moderate*), 20 risiko kategori tingkat rendah (*low*), dan 3 risiko kategori sangat rendah (*very low*). Rekomendasi mitigasi terdapat 3 klausul ISO/IEC 27001:2022 diantaranya yaitu Kontrol Sumber Daya Manusia, Kontrol Fisik, dan Kontrol Teknologi Informasi.

Kata kunci: Keamanan Informasi, Teknologi Informasi, Manajemen Risiko, OCTAVE, FMEA.

1. LATAR BELAKANG

Perkembangan teknologi informasi telah mendorong perusahaan untuk memiliki sistem pengendalian yang memadai dalam mengimplementasikan sistem berbasis teknologi. Di era digital saat ini, pemanfaatan teknologi informasi menjadi faktor penting dalam mendukung kelancaran proses bisnis. Penerapannya mencakup otomatisasi sistem, percepatan dalam pengambilan keputusan, serta peningkatan efisiensi operasional. Munculnya berbagai perusahaan berbasis teknologi informasi merupakan bentuk adaptasi terhadap kebutuhan bisnis

Received April 16, 2025; Revised April 30, 2025; Accepted Mei 24, 2025; Published: Mei 28, 2025

yang semakin kompleks serta persaingan global yang terus meningkat. Dengan demikian, teknologi informasi dimanfaatkan oleh perusahaan sebagai sarana untuk memperoleh keunggulan kompetitif, meningkatkan efisiensi, dan merespon dinamika pasar secara lebih cepat dan tepat.

Perusahaan XYZ merupakan perusahaan berbasis teknologi informasi yang mengintegrasikan *TI* dalam seluruh proses bisnisnya untuk mendukung efisiensi operasional, menawarkan solusi keuangan inovatif, serta menciptakan pengalaman digital yang optimal bagi pelanggan, khususnya lembaga keuangan mikro dan *UMKM*. Melalui berbagai layanan seperti manajemen risiko, keamanan finansial, dan pemrosesan transaksi digital, Perusahaan XYZ membantu koperasi dan lembaga keuangan bertransformasi secara digital. Hingga kini, Perusahaan XYZ telah melayani lebih dari 60 koperasi dengan produk unggulan seperti *Coopmax* dan *LPDmax*. Namun, sebagai perusahaan teknologi, Perusahaan XYZ juga menghadapi risiko keamanan informasi seperti pelanggaran data, serangan *siber*, serta kurangnya kesadaran karyawan terhadap pentingnya perlindungan data, baik dari sisi internal maupun eksternal, termasuk penyalahgunaan akses pada layanan *mobile banking*.

Terdapat beberapa penelitian terdahulu yang relevan terkait audit keamanan informasi pada perusahaan berbasis teknologi informasi. Penelitian pertama mengkaji manajemen risiko keamanan sistem informasi di *Rocketic.id* dengan pendekatan *OCTAVE* dan *FMEA*. Penelitian ini difokuskan pada situs *web Rocketic.id* dan menghasilkan temuan berupa enam risiko serta dua belas kejadian risiko yang memiliki tingkat *Risk Priority Number* (*RPN*) kategori menengah ke atas. Penelitian kedua membahas analisis keamanan situs *web* Dinas Perhubungan Provinsi Jawa Timur menggunakan metode *OCTAVE Allegro* dan *FMEA*. Proses analisis dilakukan melalui teknik wawancara untuk pengumpulan data, pengolahan data menggunakan metode *OCTAVE* dan *FMEA*, serta penilaian tingkat risiko berdasarkan nilai *RPN*. Hasil penelitian menunjukkan pengelolaan keamanan situs *web* yang sangat baik serta pencapaian tujuan keamanan yang telah ditetapkan (Setia et al., 2023). Penelitian ketiga adalah studi kasus di IT Polda Banten mengenai rencana pengamanan informasi berdasarkan analisis risiko teknologi informasi dengan pendekatan *OCTAVE* dan *ISO 27001*. Dalam penelitian tersebut, dilakukan implementasi manajemen risiko melalui identifikasi aset dan risiko menggunakan *OCTAVE*, yang diperkuat dengan metode *FMEA* untuk memperdalam analisis risiko (Anshori et al., 2019). Berdasarkan permasalahan dan temuan dalam penelitian sebelumnya, penulis menyusun analisis dan manajemen risiko keamanan sistem informasi pada

Perusahaan XYZ dengan menggunakan metode *OCTAVE* dan *FMEA* yang mengacu pada kontrol *ISO/IEC 27001:2022*.

2. KAJIAN TEORITIS

State of the art dalam penelitian ini merujuk pada kumpulan studi terdahulu yang berkaitan dengan manajemen risiko keamanan sistem informasi dengan pendekatan metode *OCTAVE*, *FMEA*, dan *ISO 27001*. Peneliti terdahulu telah melakukan berbagai evaluasi terhadap risiko sistem informasi di berbagai institusi, seperti instansi pemerintah, rumah sakit, lembaga pendidikan, dan sektor swasta. Secara umum, hasil-hasil tersebut menunjukkan bahwa metode-metode seperti *FMEA* dan *OCTAVE* cukup efektif dalam mengidentifikasi dan mengelompokkan risiko berdasarkan tingkat keparahan, kemungkinan terjadinya, dan kemudahan deteksi. Nilai *RPN (Risk Priority Number)* menjadi indikator penting dalam menentukan prioritas penanganan risiko. Terdapat pula penemuan penting seperti kebutuhan akan perbaikan sistem keamanan, peningkatan sosialisasi kebijakan keamanan, dan perlunya kontrol yang sesuai standar *ISO 27001*.

Adapun dalam berbagai studi, metode *FMEA* banyak digunakan untuk mengidentifikasi potensi kegagalan dalam sistem serta memberikan rekomendasi mitigasi sebelum risiko tersebut berdampak lebih luas. *ISO 27001* digunakan untuk memberikan kerangka kerja standar dalam manajemen keamanan informasi, sedangkan pendekatan *OCTAVE* dan variannya (seperti *OCTAVE Allegro* dan *OCTAVE-S*) digunakan untuk menilai risiko berbasis aset dan ancaman secara sistematis. Penelitian terdahulu memberikan dasar yang kuat untuk menyusun kerangka kerja dalam analisis risiko sistem informasi, sekaligus memperkuat relevansi pendekatan kombinasi metode sebagai solusi menyeluruh yang lebih komprehensif untuk menjaga keamanan sistem informasi, termasuk di dalamnya aplikasi yang digunakan oleh lembaga keuangan mikro seperti *Perusahaan XYZ*.

3. METODE PENELITIAN

Penelitian terkait dengan analisis dan manajemen risiko keamanan aset teknologi informasi dilakukan di Perusahaan XYZ yang terletak di Kecamatan Denpasar Selatan, Kota Denpasar. Penelitian ini dilakukan dengan tujuan untuk menganalisis serta mengelola risiko terhadap keamanan aset teknologi informasi pada perusahaan Perusahaan XYZ. Untuk mencapai tujuan tersebut, penelitian ini menggunakan metode kombinasi dari pendekatan *OCTAVE* (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) dan teknik

FMEA (*Failure Mode and Effect Analysis*), yang dikaji dalam kerangka kerja sistem manajemen keamanan informasi berbasis *ISO/IEC 27001:2022*.

Pendekatan *OCTAVE* dipilih karena merupakan salah satu metodologi yang berfokus pada identifikasi aset informasi yang bernilai tinggi, pengenalan terhadap ancaman serta kerentanan, dan evaluasi risiko berdasarkan konteks operasional dan strategis organisasi. *OCTAVE* memberikan keleluasaan dalam mengumpulkan informasi dari berbagai pemangku kepentingan di dalam organisasi, yang kemudian diklasifikasikan dan dianalisis untuk mengetahui tingkat risiko yang dihadapi oleh aset-aset teknologi informasi yang dimiliki.

Sementara itu, metode *FMEA* digunakan untuk memperkuat proses pengelolaan risiko dengan cara mengidentifikasi mode kegagalan potensial yang dapat terjadi terhadap aset-aset tersebut. Setiap mode kegagalan kemudian dianalisis berdasarkan tiga komponen utama, yaitu: *Severity* (tingkat keparahan dampak kegagalan), *Occurrence* (kemungkinan terjadinya kegagalan), dan *Detection* (kemampuan sistem mendeteksi kegagalan tersebut sebelum terjadi). Nilai-nilai ini kemudian digunakan untuk menghitung *Risk Priority Number* (*RPN*), yang menjadi dasar dalam penentuan prioritas tindakan mitigasi.

4. HASIL DAN PEMBAHASAN

Organizational View

Fase *Organizational View* merupakan tahap awal dalam proses identifikasi risiko dengan tujuan utama membentuk profil ancaman (*threat profile*) melalui penentuan aset penting organisasi serta kebutuhan pengamanannya. Informasi dikumpulkan dari berbagai tingkatan manajemen, mulai dari senior manajer hingga staf operasional, untuk memperoleh pemahaman menyeluruh terhadap aset, kebutuhan keamanan, potensi ancaman, serta kelemahan organisasi. Dari proses ini, dihasilkan daftar aset kritis yang mendukung proses bisnis Perusahaan XYZ, seperti server produksi, sistem manajemen pelanggan, dan jaringan internal. Selanjutnya dilakukan analisis terhadap ancaman yang paling mungkin terjadi dan dapat memberikan dampak signifikan terhadap aset penting. Tahap ini juga mencakup pendefinisian kebutuhan keamanan informasi, seperti perlindungan sistem, data, dan layanan dari ancaman serta serangkaian praktik keamanan melalui kebijakan, prosedur, dan teknologi untuk menciptakan lingkungan yang aman. Selain itu, identifikasi terhadap berbagai bentuk ancaman sistem informasi, seperti serangan siber, kesalahan konfigurasi, dan kelalaian pengguna juga dilakukan guna membantu Perusahaan XYZ mengembangkan langkah mitigasi yang tepat dalam menjaga integritas dan keamanan informasi.

Fase *Technological View*

Fase *Technological View* merupakan tahap penting dalam analisis risiko yang berfokus pada identifikasi kelemahan dari aset-aset kritis yang sebelumnya telah ditentukan. Pada fase ini, dilakukan evaluasi menyeluruh terhadap infrastruktur teknologi, sistem informasi, dan kontrol keamanan yang dimiliki oleh Perusahaan XYZ. Komponen kunci yang dianalisis terdiri dari 15 aset kritis yang terbagi dalam lima kategori utama, yaitu *hardware*, *software*, *data*, *people*, dan *network*. Analisis ini bertujuan untuk mengidentifikasi potensi kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, sehingga langkah mitigasi bisa dirancang secara tepat sasaran.

Hasil identifikasi menunjukkan berbagai kelemahan, mulai dari versi sistem operasi lama pada *production servers*, pembaruan perangkat lunak yang tidak rutin, hingga lemahnya sistem keamanan pada data penting seperti kredensial aplikasi dan database. Selain itu, kerentanan juga ditemukan pada faktor manusia seperti potensi kesalahan tim IT, serta infrastruktur jaringan yang rentan terhadap serangan jika konfigurasi keamanannya lemah. Dengan mengetahui kelemahan-kelemahan ini secara rinci, Perusahaan XYZ dapat mengembangkan kebijakan dan sistem perlindungan yang lebih kuat untuk menjaga keamanan informasi dan mengurangi risiko kerugian akibat insiden siber.

Fase *Strategy and Plan Development*

Fase *Strategy and Plan Development* merupakan tahapan penting dalam analisis manajemen risiko, di mana dilakukan identifikasi akhir sebelum masuk ke tahap penilaian risiko. Pada tahap ini, semua risiko yang telah diidentifikasi akan dianalisis berdasarkan tingkat keparahan dampaknya. Salah satu langkah konkret dalam fase ini adalah pelaksanaan pengisian kuesioner oleh staf Perusahaan XYZ yang menjadi responden untuk mengidentifikasi dan memetakan potensi risiko yang dapat mengancam aset informasi organisasi. Identifikasi risiko sendiri mencakup potensi ancaman atau kejadian yang bersumber dari lingkungan internal maupun eksternal perusahaan, yang dapat berdampak pada kinerja, keamanan, integritas, dan ketersediaan sistem informasi.

Hasil dari identifikasi risiko ini diklasifikasikan dalam berbagai kategori aset kritis seperti perangkat keras (*hardware*), perangkat lunak (*software*), data, personel (*people*), dan jaringan (*network*). Masing-masing aset tersebut memiliki potensi risiko yang berbeda-beda, dengan penyebab dan dampak yang spesifik. Sebagai contoh, pada aset perangkat keras seperti server produksi dan server pengembangan, ditemukan risiko seperti celah keamanan akibat

kurangnya konfigurasi firewall atau penggunaan login tanpa SSH key, yang berpotensi menyebabkan serangan malware atau gangguan layanan. Risiko serupa juga ditemukan dalam perangkat lunak inti, di mana kerentanan sistem dapat menyebabkan pencurian data atau gangguan operasional. Selain itu, risiko juga muncul dari aspek manusia, seperti kesalahan konfigurasi oleh tim IT, kurangnya kesadaran keamanan, hingga ketidaktepatan dalam proses offboarding yang dapat menyebabkan akses tidak sah ke sumber daya perusahaan.

Setelah risiko teridentifikasi, langkah selanjutnya adalah analisis penilaian risiko menggunakan metode *Failure Mode and Effect Analysis* (FMEA). Penilaian ini mencakup tiga parameter utama: *Severity* (tingkat keparahan), *Occurrence* (frekuensi kejadian), dan *Detection* (kemampuan deteksi risiko). Nilai dari ketiga parameter ini diberikan melalui kuesioner yang diisi oleh responden, kemudian dihitung untuk mendapatkan nilai *Risk Priority Number* (RPN) sebagai acuan dalam prioritas penanganan risiko.

Tabel 1. Hasil Analisis Penilaian Kuesioner FMEA

Asset	Penyebab Potensial	Risiko	SEV	OCC	DEC	RPN	LEVEL	Tingkatan Risiko
Development Servers	Adanya celah keamanan	Pengambilan akses	8	2	6	96	Medium	**7**
	Tidak update server	Mudah diretas	7	3	3	63	Low	**16**
	Tidak melakukan konfigurasi firewall	Serangan malware	7	2	4	56	Low	**19**
	Manajemen akses yang kurang terkontrol	Penyalahgunaan akses	6	2	5	60	Low	**18**
Production Servers	Ketidaksempurnaan pemeliharaan dan konfigurasi	Akses tidak sah, penurunan kinerja server dan biaya tambahan karena pemulihan darurat	10	3	6	180	High	**1**
Laptop & Computers	Serangan fisik terhadap komputer	Kerusakan atau pencurian perangkat keras dapat mengakibatkan hilangnya data sensitif, kebocoran informasi pengguna, atau ketidaktersediaan sistem	7	2	5	70	Low	**12**
Core Applications	Kerentanan keamanan yang tidak terdeteksi	Pengambilan akses dan penyusupan	10	2	5	100	Medium	**6**
	Minimnya fasilitas atau	Kekurangan informasi untuk						

	fitur untuk melakukan audit penggunaan sistem	investigasi keamanan	6	3	5	90	Medium	**9**
	Konfigurasi sistem yang tidak sesuai atau tidak akurat	Kebocoran informasi rahasia ke pihak tidak berkepentingan	8	2	4	64	Low	**15**
	Manajemen akses yang tidak mumpuni	Kegagalan manajemen hak akses pengguna	9	2	3	54	Low	**25**
Website and Domains	Tidak menggunakan SSL	Mudah diretas	8	2	2	32	Low	**28**
	Tidak update dan tidak perpanjang domain	Phising dan pencurian domain	9	2	3	54	Low	**21**
Application Credentials	Akun bersama	Penyalahgunaan akses	7	4	6	168	High	**2**
	Kelemahan kata sandi	Pemalsuan identitas	9	2	7	126	High	**3**
	Data sensitif	Kompromi data sensitif	8	3	5	120	High	**4**
Application Logs	Record akses secara public	Pencurian identitas	7	2	4	56	Low	**20**
	Data sensitif	Pengungkapan kerentanan aplikasi	8	2	4	64	Low	**13**
Applications Source Codes	Repository GitHub terpublikasi	Risiko pada proyek terkait dan hilangnya kendali pengembangan	8	1	4	32	Low	**29**
	Insider sabotage	Kehilangan kerahasiaan kode sumber dan penyalahgunaan data	9	1	6	54	Low	**22**
Application Database	Keamanan lemah	Akses tidak sah	10	2	6	120	High	**5**
	Insider sabotage	Pencurian dan manipulasi data	10	1	6	60	Low	**17**
Financial Data	Kontrol akses aplikasi lemah	Akses tidak sah dan penyalahgunaan keuangan	5	2	3	30	Low	**30**
	Penyimpanan dokumen fisik tidak terjaga dengan baik	Pencurian identitas dan kredensial keuangan	5	2	4	40	Low	**26**
Software Licenses	Akses tidak sah oleh pihak internal atau eksternal yang tidak berwenang	Penggunaan lisensi tidak sah dan gangguan operasional	6	2	4	48	Low	**24**
Internal Application Accounts & Access	Kurangnya verifikasi identitas	Pencurian informasi dan serangan insider	5	2	4	40	Low	**27**
	Manajemen akses yang tidak tepat	Akses tidak sah ke data sensitif	8	2	4	64	Low	**14**
Tim IT	Kesalahan	Kerugian finansial, kerugia n reputasi, dan	8	3	4	96	Medium	**8**

	manusia dalam pengembangan atau konfigurasi sistem	ketidaktersediaan layanan bagi pengguna aplikasi.						
	Minimnya proses screening dalam setiap proses rekrutmen pegawai baru	Sabotase dan kebocoran data oleh karyawan bermotif jahat	7	3	4	84	Medium	**10**
	Rendahnya kesadaran keamanan akses sumber daya perusahaan	Risiko serangan malware pada perangkat/akun pegawai mengancam data perusahaan	8	2	5	80	Medium	**11**
	Kelalaian penghapusan hak akses dalam offboarding	Risiko akses ilegal dan penyalahgunaan data	9	2	3	54	Low	**23**
Router	Ketidakamanan konfigurasi	Penyusupan jaringan	5	1	3	15	Very Low	**32**
	Manajemen kata sandi lemah	Eksploitasi celah keamanan	5	1	3	15	Very Low	**33**
Access point	Konfigurasi yang tidak aman	Penyadapan data	5	1	3	15	Very Low	**34**
	Kurangnya enkripsi	Pencurian kredensial dan pemalsuan identitas	6	1	4	24	Low	**31**

Hasil analisis nilai RPN menunjukkan tingkat risiko yang dikategorikan berdasarkan rentang nilai sesuai dengan skala prioritas FMEA. Kategori sangat rendah (*Very Low*), yang direpresentasikan dengan warna hijau dan berada pada rentang nilai RPN 0-20, mencakup 3 ancaman risiko. Kategori rendah (*Low*), yang ditandai dengan warna biru dan berada pada rentang nilai RPN 20-80, mencakup 20 ancaman risiko. Selanjutnya, kategori sedang (*Moderate*), yang diidentifikasi dengan warna kuning dan berada pada rentang nilai RPN 80-120, mencakup 6 ancaman risiko. Untuk kategori tinggi (*High*), yang digambarkan dengan warna jingga pada rentang nilai RPN 120- 200, terdapat 5 ancaman risiko. Tidak ditemukan ancaman yang masuk dalam kategori sangat tinggi (*Very High*), yang memiliki rentang nilai lebih dari 200, termasuk pada risiko yang teridentifikasi dalam aset Perusahaan XYZ.

Hasil evaluasi risiko pada tabel menunjukkan terdapat 11 risiko dengan level "*High*" dan "*Medium*" yang mendapatkan rekomendasi penanganan. Level risiko ditentukan berdasarkan nilai RPN (*Risk Priority Number*) yang dihitung dari tingkat keparahan (*Severity*), kemungkinan kejadian (*Occurrence*), dan kemampuan deteksi (*Detection*). Risiko dengan level *Medium* memiliki nilai RPN antara 80-120, sedangkan *High* berkisar antara 120-200. Dalam kasus ini, tidak ditemukan risiko dengan level "*Very High*" (RPN > 200). Risiko yang

mendapatkan rekomendasi diprioritaskan berdasarkan dampaknya yang signifikan terhadap keamanan sistem, data sensitif, dan operasional bisnis, dengan mempertimbangkan tingkat keparahan tinggi, frekuensi kejadian sedang hingga tinggi, serta rendahnya kemampuan deteksi. Risiko dengan level "*Low*" tidak diberikan rekomendasi karena dianggap memiliki dampak yang minimal dan dapat diterima tanpa tindakan mitigasi lebih lanjut.

Rekomendasi Mitigasi Standar ISO/IEC 27001:2022

Pada tahap ini dilakukannya analisis mengenai manajemen risiko keamanan informasi yaitu *menggunakan Failure Mode And Effect Analysis* (FMEA) di Perusahaan XYZ, selanjutnya dilakukan pemetaan pemilihan klausul dan kontrol keamanan untuk rekomendasi mitigasi risiko menggunakan standar ISO/IEC 27001:2022 yang disesuaikan dengan risiko yang terjadi di Perusahaan XYZ yaitu perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia (*people*), jaringan (*network*), dan data (*data*).

Terdapat 16 rekomendasi penanganan risiko yang diusulkan untuk Perusahaan XYZ, yang dikategorikan berdasarkan tiga klausul utama dalam ISO/IEC 27001:2022, yaitu: klausul 6 (kontrol orang) yang mencakup pelatihan keamanan informasi, proses rekrutmen yang aman, dan penetapan tanggung jawab dalam perjanjian kerja; klausul 7 (kontrol fisik) yang mencakup perlindungan fisik terhadap ancaman lingkungan, serta pengamanan perangkat IT dari akses tidak sah; dan klausul 8 (kontrol teknologi) yang berfokus pada pengamanan teknologi seperti penggunaan autentikasi dua faktor, manajemen kerentanan teknis, enkripsi data, serta penerapan firewall dan sistem deteksi intrusi. Setiap rekomendasi dirancang untuk mengatasi risiko spesifik yang diidentifikasi, dengan tujuan mengurangi potensi dampak yang dapat merugikan operasional Perusahaan XYZ dan memastikan kepatuhan terhadap standar keamanan informasi yang berlaku.

Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) di Perusahaan XYZ dirancang berdasarkan standar ISO/IEC 27001:2022 dengan mengidentifikasi dan menyesuaikan kontrol dari tingkat tertinggi hingga terendah untuk mitigasi risiko. Tiga pilar utama dari SMKI mencakup kontrol terhadap orang, fisik, dan teknologi. Kontrol terhadap orang bertujuan mencegah ancaman dari individu yang tidak berwenang dan menanamkan budaya keamanan informasi sejak awal masa kerja. Ruang lingkup kebijakan ini mencakup tahap sebelum dan selama bekerja, seperti proses skrining latar belakang, kontrak kerja dengan klausul keamanan informasi, serta pelatihan dan peningkatan kesadaran secara berkala bagi karyawan.

Pendekatan ini memastikan bahwa seluruh SDM memahami dan menjalankan peran aktif dalam menjaga keamanan aset informasi organisasi.

Sementara itu, kontrol fisik difokuskan untuk mencegah akses tidak sah ke fasilitas organisasi dan melindungi peralatan dari kerusakan maupun gangguan. Hal ini mencakup pengamanan area kerja terhadap bencana maupun tindakan sabotase, serta memastikan ketersediaan utilitas pendukung seperti pasokan daya. Di sisi lain, kontrol teknologi mencakup keamanan akses dan autentikasi, manajemen konfigurasi, dan keamanan jaringan. Kebijakan ini memastikan bahwa hanya personel berwenang yang dapat mengakses informasi sensitif, konfigurasi sistem dilakukan secara konsisten dan aman, serta jaringan organisasi terlindungi dari serangan internal dan eksternal. Implementasi meliputi autentikasi yang aman, pembatasan hak akses, pencegahan kebocoran data, penyamaran data (*masking*), serta pengelolaan kerentanan dan audit sistem informasi secara terencana. Dengan struktur yang menyeluruh ini, Perusahaan XYZ menargetkan terciptanya sistem keamanan informasi yang kuat dan berkelanjutan.

5. KESIMPULAN DAN SARAN

Penelitian ini bertujuan untuk mengevaluasi manajemen keamanan aset teknologi informasi di Perusahaan XYZ dengan menggunakan metode *OCTAVE* dan *FMEA*. Hasil penelitian menunjukkan bahwa Perusahaan XYZ memiliki sejumlah aset kritis yang memerlukan perlindungan lebih lanjut serta menghadapi berbagai risiko keamanan yang signifikan. Melalui analisis tiga fase dalam metode *OCTAVE*, berhasil diidentifikasi 15 kategori aset penting serta 34 risiko utama yang mencakup kerentanan yang tidak terdeteksi, pemeliharaan dan konfigurasi yang belum optimal, serta rendahnya kesadaran keamanan di kalangan karyawan. Selanjutnya, metode *FMEA* digunakan untuk menilai tingkat keparahan risiko tersebut, yang menghasilkan klasifikasi ke dalam empat tingkatan: 5 risiko pada level *High*, 6 pada *Medium*, 20 pada *Low*, dan 3 pada *Very Low*, dengan nilai *Risk Priority Number (RPN)* tertinggi sebesar 180 pada aset *Production Servers* dan terendah sebesar 15 pada *Access Point*. Sebagai pelengkap, penerapan standar *ISO/IEC 27001:2022* menjadi kerangka kerja yang mendukung pengelolaan risiko secara menyeluruh, di mana dihasilkan 16 rekomendasi penanganan untuk 11 aset teridentifikasi, yang mengacu pada klausul 6 mengenai kontrol sumber daya manusia, klausul 7 terkait kontrol fisik, dan klausul 8 mengenai kontrol teknologi. Pendekatan ini memperkuat upaya perlindungan terhadap aset informasi dan meningkatkan kesiapan Perusahaan XYZ dalam menghadapi potensi ancaman keamanan siber.

Peneliti memberikan beberapa saran yang dapat dijadikan acuan untuk pengembangan selanjutnya. Pertama, disarankan agar penelitian mendatang mengeksplorasi pendekatan alternatif dalam analisis dan manajemen risiko keamanan informasi, seperti *NIST CSF* atau *COSO*, guna memberikan perspektif perbandingan terhadap efektivitas metode *FMEA* dan standar *ISO/IEC 27001:2022*. Kedua, ruang lingkup identifikasi aset dan analisis risiko sebaiknya diperluas, tidak terbatas pada aspek teknologi informasi saja, agar memberikan gambaran risiko yang lebih menyeluruh. Terakhir, perusahaan diharapkan segera mengimplementasikan rekomendasi mitigasi risiko yang telah disusun, agar efektivitas analisis risiko dapat dievaluasi dan tujuan keamanan informasi di Perusahaan XYZ dapat tercapai secara optimal.

UCAPAN TERIMA KASIH

Saya mengucapkan terima kasih yang sebesar-besarnya kepada Ibu Ni Made Ika Marini Mandenni dan Bapak Muhammad Alam Pasirulloh atas segala bimbingan dan arahan yang telah diberikan selama penyusunan tugas akhir ini. Ucapan terima kasih juga saya sampaikan kepada Bapak Arya Maharta selaku *Chief Technology Officer* serta seluruh staf Perusahaan XYZ yang telah memberikan dukungan dan bantuan selama pelaksanaan penelitian.

DAFTAR REFERENSI

Anshori, F. A., Suprapto, S., & Perdanakusuma, A. R. (2019). Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(2), 1701–1707. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/4551

Fadilla, I., Sartika, N., & Bisma, R. (2021). *Perancangan Sistem Informasi Manajemen Risiko berdasarkan ISO 27001 : 2013 (Sistem Manajemen Keamanan Informasi)*. *02*(03), 81–86.

Handayani, N. U., Wibowo, M. A., Sari, D. P., Satria, Y., & Gifari, A. R. (2018). Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001. *TEKNIK*, *39*(2), 78–85. https://doi.org/10.14710/TEKNIK.V39I2.15918

hanifah, P. (puja), & Suroso, J. S. (Jarot). (2020). Analisis Risiko Sistem Informasi pada RSIA Eria Bunda Menggunakan Metode FMEA. *Jurnal Komputer Terapan*, *6*(2), 210–221. https://doi.org/10.35143/JKT.V6I2.3728

Islam, U., Ampel, N. S., Surabaya, S., & Timur, J. (2021). Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013. *Technomedia Journal*, *5*(2 Februari), 167–181. https://doi.org/10.33050/TMJ.V5I2.1377

Mutiah, N., Rusi, I., Sistem Informasi, J., & MIPA UniversitasTanjungpura Jalan Hadari Nawawi, F. H. (2022). Analisis dan Manajemen Risiko Keamanan Informasi Menggunakan Metode Failure Mode And Effects Analysis (FMEA) Dan Kontrol ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Sambas). *Coding Jurnal Komputer Dan Aplikasi*, *10*(02), 249–261. https://doi.org/10.26418/CODING.V10I02.55082

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. https://doi.org/10.30865/JURIKOM.V10I2.5950

Puspita Ningsih, K., Tunnisa, U., Erviana, N., Rekam Medis dan Informasi Kesehatan, P., Jenderal Ahmad Yani, U., Jl Brawijaya, I., Barat, R., & Korespondensi, I. (2020). Manajemen Resiko Redesign Sistem Penjajaran Rekam Medis dengan Metode Failure Mode and Effect Analysis (FMEA). *Indonesian of Health Information Management Journal (INOHIM)*, *8*(1), 08–20. https://doi.org/10.47007/INOHIM.V8I1.204

Rohman, A. F., Ambarwati, A., & Setiawan, E. (2020). Analisis Manajemen Risiko IT dan Keamanan Aset Menggunakan Metode Octave-S. *INTECOMS: Journal of Information Technology and Computer Science*, *3*(2), 298–310. https://doi.org/10.31539/INTECOMS.V3I2.1854

Rosmiati, I., & Kuraesin, A. D. (2021). Pengaruh Struktur Organisasi Terhadap Kualitas Sistem Informasi Akuntansi Pada Pt. Kunci Inti Transindo Jakarta. *Jurnal Ilmiah Akuntansi Kesatuan*, *9*(2), 389–398. https://doi.org/10.37641/jiakes.v9i2.875

Setia, H. A., Safitri, E. M., Putri, V. R., & Wibowo, C. P. (2023). Analisis Keamanan Website Dinas Perhubungan Provinsi Jawa Timur Menggunakan Metode Octave Allegro dan FMEA. *Prosiding*

Surya, M., Setiawan, A., Safitri, E. M., Asyam, M., Taufiqurahman, T., & Pratama, M. A. (2023). Analisis Manajemen Risiko Keamanan Sistem Informasi Rocketic.id menggunakan Metode OCTAVE dan FMEA. *JUSTIN (Jurnal Sistem Dan Teknologi Informasi)*, *11*(3), 504–514. https://doi.org/10.26418/JUSTIN.V11I3.66628