ISSN: 2598-8565 (media cetak)
ISSN: 2620-4339 (media online)

ANALISIS MANAJEMEN RISIKO ASET TEKNOLOGI INFORMASI PADA PERUSAHAAN SISTEM INTEGRATOR DENGAN MENGGUNAKAN METODE *OCTAVE ALLEGRO*

Amelia Dwi Indriani✉, Tristyanti Yunitasari
Manajemen Sistem Informasi, Universitas Gunadarma, Depok, Indonesia
Email: ameliaadrn@gmail.com

DOI: https://doi.org/10.46880/jmika.Vol9No2.pp238-254

ABSTRACT

The Utilization of Information Technology frequently carries significant security risks, both from external threats such as cyber-attacks (viruses, malware, phishing, ransomware) and from internal factors such as human error. This research aims to identify, assess, and mitigate the risks of information technology assets in an Indonesian system integrator company using the OCTAVE Allegro method. This method was chosen because it focuses on critical information assets and provides a structured approach through eight steps in four phases of analysis. The results of the study show that there are four critical assets in the company's information technology, namely hardware, software, data and information, as well as access rights and credentials. Based on the risk assessment matrix, data and information assets have the highest risk score with an average of 38.8, followed by access rights and credentials (38), software (37.42), and hardware (36.33). All risk categories are in POOL 1, which means they require immediate mitigation measures. Consistent implementation of risk management is expected to strengthen the company's resilience to information security threats and also enhance its reputation and competitiveness in the technology industry.

Keyword: Risk Management, OCTAVE Allegro, System Integrator, Information Technology, Information Security.

ABSTRAK

Pemanfaatan teknologi informasi seringkali membawa risiko keamanan yang signifikan, baik dari ancaman eksternal seperti serangan siber (virus, malware, phishing, ransomware) maupun dari faktor internal seperti human error. Penelitian ini bertujuan untuk mengidentifikasi, menilai, dan memitigasi risiko aset teknologi informasi pada sebuah perusahaan sistem integrator di Indonesia dengan menggunakan metode OCTAVE Allegro. Metode ini dipilih karena fokus pada aset informasi kritis dan memberikan pendekatan terstruktur melalui delapan langkah dalam empat fase analisis. Hasil penelitian menunjukkan bahwa terdapat empat aset kritis dalam Teknologi Informasi perusahaan, yaitu hardware, software, data dan informasi, serta hak akses dan kredensial. Berdasarkan matriks penilaian risiko, aset data dan informasi memiliki skor risiko tertinggi dengan rata-rata 38,8, diikuti oleh hak akses dan kredensial (38), software (37,42), dan hardware (36,33). Seluruh kategori risiko berada pada POOL 1, yang berarti membutuhkan langkah mitigasi segera. Implementasi manajemen risiko yang konsisten diharapkan dapat memperkuat ketahanan perusahaan terhadap ancaman keamanan informasi dan juga meningkatkan reputasi serta daya saing di industri teknologi.

Kata Kunci: Manajemen Risiko, OCTAVE Allegro, Sistem Integrator, Teknologi Informasi, Keamanan Informasi.

PENDAHULUAN

Sumber daya sistem informasi yang mencakup perangkat keras (*hardware*), perangkat lunak (*software*), manusia (*user*), data, dan peralatan pendukung lainnya merupakan aset vital bagi organisasi yang harus dilindungi dari risiko keamanan baik dari internal maupun eksternal organisasi. Untuk itu dibutuhkan pemahaman organisasi mengenai keamanan informasi terkait apa yang harus dilindungi dan bagaimana solusi yang tepat dalam menangani permasalahan terkait keamanan informasi. Tujuan dari sistem informasi keamanan adalah untuk menjamin kelanjutan proses bisnis, mengurangi resiko bisnis, dan meningkatkan return of investment (ROI) serta peluang bisnis (Prasetyaningrum et al, 2022). Selain itu adanya risiko yang akan terjadi karena dipengaruhi oleh faktor kemungkinan berupa ancaman seperti kegagalan kelistrikan karena faktor alam, human error, ancaman

IT seperti virus dan malware karena hacker, dan lain sebagainya akan memberikan dampak yang bisa merugikan organisasi/perusahaan. Risiko tersebut dapat dikendalikan menggunakan manajemen risiko.

Manajemen risiko adalah suatu pendekatan terstruktur dalam proses identifikasi, analisis, perencanaan, dan pengendalian risiko dalam suatu organisasi. Tujuannya adalah untuk mengurangi dampak dari kejadian yang merugikan serta meningkatkan peluang untuk memaksimalkan potensi keuntungan (Kristiana, et al, 2022). Analisis risiko yang adalah bagian dari manajemen risiko yang berorientasi pada identifikasi, penilaian, dan pemahaman tingkat risiko yang mungkin terjadi. Dengan melakukan analisis risiko, organisasi/perusahaan dapat membuat langkah-langkah strategis untuk melakukan penanganan terhadap risiko yang mungkin terjadi serta lebih siap dalam menghadapi dampak yang timbul dari risiko yang terjadi.

Penelitian ini melibatkan salah satu perusahaan Sistem Integrator di Indonesia. Secara garis besar perusahaan ini bergerak di industri teknologi yang secara khusus melakukan penggabungan berbagai komponen teknologi, perangkat lunak, perangkat keras, dan sistem yang berbeda agar dapat bekerja secara terpadu sebagai satu solusi yang efisien. Umumnya Sistem Integrator memiliki rekanan atau kerja sama dengan berbagai vendor teknologi seperti Microsoft, Cisco, Oracle, dan lainnya untuk memberikan solusi untuk klien perusahaan tersebut. Sebagai penyedia layanan Teknologi Informasi, tentunya secara operasional perusahaan memanfaatkan TIK dalam setiap kegiatan bisnis yang sedang berjalan. Dalam implementasinya, tidak menutup kemungkinan adanya peningkatan terhadap kerentanan dari serangan siber seperti virus, malware, phishing, ransomware, dan pelanggaran lain yang dapat menimbulkan kerugian. Untuk itu Perusahaan Sistem Integrator ini perlu menerapkan langkah-langkah keamanan untuk melindungi data sensitif dan mencegah akses yang tidak sah. Permasalahan lain yaitu kesalahan dari manusia baik disengaja ataupun tidak disengaja dapat meningkatkan kerentanan keamanan. Dalam hal ini perusahaan harus mematuhi berbagai regulasi dan standar industri terkait keamanan sistem informasi.

Penelitian ini bertujuan untuk melakukan pengukuran dan identifikasi risiko yang tepat terhadap Perusahaan Sistem Integrator. Tentu perusahaan memiliki aset informasi seperti hardware, software, hingga manusia yang wajib dilindungi dari ancaman dan risiko keamanan baik dari internal maupun eksternal perusahaan. Keberhasilan dalam mengelola risiko dengan metode OCTAVE Allegro dapat menciptakan ketahanan perusahaan terhadap ancaman dan menjaga kelangsungan bisnis. Selain itu dapat meningkatkan reputasi perusahaan sebagai entitas yang dapat diandalkan untuk menjaga keamanan data dan informasi.

TINJAUAN PUSTAKA

Aset Informasi

Informasi dalam bentuk apapun merupakan suatu aset yang berharga bagi organisasi atau perusahaan dan saat ini dikategorikan sebagai "aset informasi" (Fathullah & Subbarao, 2022). Sebagian informasi yang dimiliki organisasi dapat meninggalkan jejak digital yang berpotensi dimanfaatkan oleh pihak eksternal, khususnya kompetitor. Oleh karena itu, informasi tersebut perlu dilindungi dari akses publik. Kondisi ini mendorong peningkatan jumlah aset informasi sekaligus memperluas cakupan risiko yang mengancamnya. Akibatnya, timbul tantangan baru dalam perlindungan aset informasi, seperti pembajakan dan pelanggaran hak kekayaan intelektual, sehingga diperlukan analisis risiko keamanan yang sistematis serta langkah pencegahan untuk menghadapi potensi insiden (Abdullah, et al 2021). Untuk melakukan analisis risiko, perlu adanya proses klasifikasi aset informasi. Dimana aset informasi akan dikelompokkan berdasarkan nilai, sensitivitas, dan pentingnya bagi organisasi. Ini membantu organisasi dalam mengelola risiko keamanan informasi dengan fokus pada perlindungan aset yang paling berharga atau kritis.

Keamanan Informasi

Keamanan informasi dapat diartikan sebagai suatu cara dalam menjaga kerahasiaan, integritas, dan ketersediaan dari informasi dimana memiliki tujuan untuk melindungi aset informasi berharga dari pengungkapan, modifikasi, atau penghancuran yang tidak sah(Pardosi, et al 2024). Prinsip keamanan informasi dalam ISO 27001, yang dikenal sebagai CIA Triad, merupakan fondasi utama dalam manajemen keamanan informasi. Konsep ini berfungsi sebagai kerangka acuan yang dapat digunakan individu maupun organisasi dalam merancang aplikasi, sistem, prosedur, atau kebijakan yang berkaitan dengan perlindungan informasi (Harahap et al, 2023).

Metode OCTAVE *Allegro*

OCTAVE *Allegro* merupakan seperangkat alat, teknik, dan metode yang digunakan untuk menilai serta merencanakan keamanan teknologi informasi berbasis

risiko. kata allegro berasal dari bahasa Italia yang berarti cepat dan lincah, sehingga mencerminkan kinerja OCTAVE Allegro yang responsif dan efisien (Emmanuel & Maulany, 2023). Salah satu keunggulan OCTAVE Allegro adalah fleksibilitasnya, sehingga dapat digunakan baik oleh individu maupun organisasi untuk melakukan penilaian risiko yang komprehensif, bahkan tanpa melibatkan banyak pihak atau sumber daya yang luas.

Pada penelitian sebelumnya (Khotimah et al., 2021) dengan judul Analisis dan Manajemen Risiko Keamanan Informasi pada Rumah Sakit Menggunakan Metode Octave Allegro (Studi Kasus: Rumah Sakit Umum Daerah Cengkareng). Penelitian ini menggunakan metode OCTAVE Allegro untuk menganalisis dan memberikan mitigasi risiko terhadap aset informasi di RSUD Cengkareng. Dari hasil identifikasi, ditemukan 8 area risiko utama yang berdampak pada reputasi, keuangan, produktivitas, keselamatan, dan aspek hukum. Rekomendasi mitigasi disusun berdasarkan tingkat risiko yang tinggi dalam relative risk matrix, seperti kerusakan data pengguna dalam database rumah sakit. Evaluasi berkala terhadap keamanan sistem informasi juga diperlukan guna menjaga keberlangsungan dan keandalan layanan rumah sakit.

Serta pada penelitian (Anwar et al., 2024) yang berjudul Mitigasi Risiko Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Berbasis Manajemen Risiko OCTAVE Allegro di Perguruan Tinggi : Studi kasus Perguruan Tinggi x. Penelitian ini mengevaluasi risiko keamanan informasi pada sistem informasi akademik di Perguruan Tinggi X dan menemukan 10 risiko kategori rendah, 5 risiko sedang, dan 4 risiko tinggi, serta menghasilkan 47 rekomendasi pengendalian berdasarkan Annex A SNI ISO/IEC 27001:2013. Penelitian merekomendasikan agar unit TI mulai menerapkan manajemen risiko keamanan informasi secara berkala dan melanjutkan rencana SMPI ke tahap implementasi untuk memperkuat sistem keamanan informasi di lingkungan akademik.

METODE PENELITIAN

Pada penelitian ini diawali dengan melakukan perencanaan, kegiatan yang dilakukan adalah sebagai berikut: studi literatur, menentukan objek penelitian, menentukan data yang dibutuhkan.

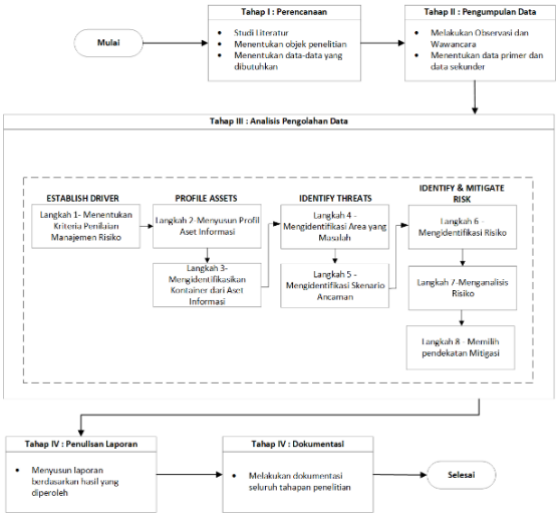
Objek penelitian pada penelitian ini adalah perusahaan teknologi yang berfokus pada bidang Sistem Integrator di Jakarta.

Teknik pengumpulan data yang digunakan ialah dengan observasi, wawancara, dokumen yang berkaitan dengan penelitian. Wawancara dilakukan melalui purposive sampling kepada narasumber dengan kriteria:

- Narasumber harus memiliki tanggung jawab atau pengalaman langsung dalam mengelola aset informasi, baik dari sisi teknis maupun manajerial
- Narasumber memiliki otoritas atau akses terhadap informasi terkait inventaris aset, laporan insiden, SOP, maupun dokumen kebijakan internal.
- Narasumber sudah bekerja lebih dari 10 tahun di perusahaan tersebut

Berdasarkan kriteria tersebut, Manager IT Infrastruktur yang memenuhi data untuk menggambarkan apa yang menjadi tujuan dan permasalahan dari penelitian ini.

Teknik analisis menggunakan metode Octave Allegro. Metode ini lebih praktis, fokus pada aset informasi, dan mampu menghubungkan risiko teknis dengan dampak bisnis.



Gambar 1. *Flowchart* Tahapan Penelitian

HASIL DAN PEMBAHASAN

Fase I: Establish Drivers

Dalam metode OCTAVE Allegro, terdapat lima area dampak utama yang harus dipertimbangkan, yaitu reputasi dan kepercayaan pelanggan, keuangan, produktivitas, keselamatan dan kesehatan, serta denda dan sanksi hukum. Area dampak ini dapat disesuaikan atau dimodifikasi sesuai dengan kebutuhan organisasi.

Tabel 1. Prioritas Area Dampak

Allegro Worksheet	***Impact Area Prioritization Worksheet***
Prioritas	**Area Dampak**

5	Reputasi dan Kepercayaan Pelanggan
4	Keuangan
3	Produktivitas
2	Denda dan Sanksi Hukum
1	Keselamatan dan Kesehatan
N/A	Ditentukan Pengguna

Berdasarkan Tabel 1, urutan prioritas area dampak ditentukan oleh responden melalui wawancara, responden memilih Reputasi sebagai area dampak dengan skor prioritas tertinggi karena bagi perusahaan sistem integrator, reputasi dan kepercayaan pelanggan adalah aset paling berharga. Bisnis yang dijalankan sangat bergantung pada proyek dan hubungan jangka panjang. Jika reputasi rusak, pelanggan akan kehilangan kepercayaan dan beralih ke kompetitor. Hal ini tidak hanya memengaruhi satu proyek, tapi juga menghancurkan potensi bisnis di masa depan. Sebuah kesalahan kecil bisa menyebar dengan cepat dan merusak citra perusahaan secara permanen. Oleh karena itu, area ini dinilai sebagai dampak tertinggi. Untuk Kerugian finansial tentu menjadi dampak yang sangat penting. Namun, dalam bisnis sistem integrator, kerugian finansial seringkali merupakan konsekuensi dari kegagalan di area lain. Misalnya, reputasi yang buruk dapat menyebabkan hilangnya proyek besar, yang secara langsung berdampak pada keuangan. Denda atau sanksi hukum juga akan berujung pada kerugian finansial. Jadi, meskipun keuangan adalah pilar utama, seringkali ia menjadi cerminan dari kegagalan di area-area lain. Produktivitas yang menurun dapat memperlambat pengerjaan proyek, meningkatkan biaya, dan menyebabkan keterlambatan. Hal ini bisa berdampak pada kepuasan pelanggan dan, pada akhirnya, merugikan secara finansial. Denda dan sanksi hukum bisa sangat merugikan secara finansial. Namun, kasus seperti ini biasanya terjadi akibat kegagalan untuk mematuhi regulasi atau kontrak. Meskipun penting, kejadian ini seringkali spesifik untuk kasus tertentu dan tidak selalu mencerminkan kesehatan operasional perusahaan secara keseluruhan. Dan yang terakhir Meskipun keselamatan dan kesehatan sangat krusial dan tidak bisa dinegosiasikan, dalam konteks bisnis sistem integrator, risiko ini seringkali lebih kecil dibandingkan industri yang memiliki bahaya fisik tinggi (misalnya, konstruksi atau manufaktur berat). Risiko yang terkait dengan cedera fisik atau kecelakaan kerja biasanya lebih rendah. Oleh karena itu, dalam konteks prioritas dampak bisnis secara keseluruhan, area ini ditempatkan pada urutan terakhir.

Fase II: Profile Assets

Setelah menetapkan kriteria pengukuran risiko untuk, akan dilanjutkan untuk fase kedua yaitu melakukan profiling terhadap aset informasi dan melakukan identifikasi kontainer aset informasi.

Tabel 2. *Information Asset Risk Environment Map (Technical)*

Allegro Worksheet	***Information Asset Risk Environment Map (Technical)***
Internal	
Deskripsi Kontainer	***Owner (s)***
- Server - Storage - Komputer karyawan - Laptop - Perangkat jaringan (switch, router, access point), Printer, Scanner - CCTV - Flat panel meeting room	Divisi IT Infrastruktur
- SAP Business One (perangkat lunak manajemen bisnis (ERP) - Success Factor (Perangkat lunak personalia) - Salesforce - Microsoft Exchange - Office 365 - Microsoft Teams - Microsoft SQL - Power BI - Freshwork - Trello - Sharepoint	Divisi IT Infrastruktur
- Data pelanggan - Data karyawan - Data keuangan - Data operasional - Data warehouse - Dokumen kontrak - Dokumen legal	Divisi Data/Legal/HR/Finance
- Akun pengguna - Autentikasi pengguna - Sertifikat digital	Divisi IT Security
Eksternal	
Deskripsi Kontainer	***Owner* (s)**
Internet	Vendor Telekomunikasi

Hosting DNS/Cloud	Domain Provider
Salesforce, Office 365, Trello, Freshwork, Sharepoint (cloud version)	Provider Layanan

Pada tabel 2 diatas menjelaskan tentang peta lingkungan aset informasi secara teknikal yang memiliki keterkaitan dengan proses yang dilakukan secara teknik yang dijalankan untuk mendukung pengolahan data dan komunikasi.

Tabel 3. *Information Asset Risk Environment Map (Physical)*

Allegro Worksheet	***Information Asset Risk Environment Map (Physical)***
Internal	
Deskripsi Kontainer	***Owner (s)***
- Server - Storage - Komputer karyawan - Laptop - Perangkat jaringan (switch, router, access point), Printer, Scanner - CCTV - Flat panel meeting room	Divisi IT Infrastruktur
- Dokumen Fisik : Dokumen kontrak, Dokumen Legal, Dokumen Keuangan, dan Dokumen Pelanggan	Divisi Terkait seperti Legal/HR
Eksternal	
Deskripsi Kontainer	***Owner (s)***
Copy Dokumen Fisik	Mitra Eksternal

Peta Lingkungan Aset Informasi Fisik menggambarkan aset-aset yang terkait langsung dengan infrastruktur fisik yang mendukung operasional sistem informasi perusahaan.

Tabel 4. *Information Asset Risk Envirotment Map (People)*

Allegro Worksheet	***Information Asset Risk Environment Map (People)***
Internal	
Deskripsi Kontainer	***Owner (s)***
Karyawan Perusahaan	Perusahaan Sistem Integrator
Manajemen Perusahaan	
Divisi IT	
External	
Deskripsi Kontainer	***Owner (s)***
Mitra Bisnis	Mitra Eksternal
Prinsipal : Prinsipal atau produsen adalah pemilik brand dari produk yang didistribusikan oleh distributor.	Prinsipal

Peta Lingkungan Aset Informasi Manusia (People) pada Tabel 4 merupakan aset berupa individu atau kelompok yang berinteraksi dengan aset informasi. Peran mereka penting karena mereka adalah pengguna, pengelola, dan terkadang juga menjadi ancaman bagi keamanan informasi. Memahami aset people membantu organisasi mengelola risiko terkait perilaku dan otorisasi manusia.

Fase III: Identify Threats

Fase selanjutnya adalah identifikasi ancaman (Identify Threats) berfokus pada upaya menemukan berbagai potensi ancaman yang dapat memengaruhi aset informasi. Fase ketiga ini terdiri dari dua tahapan yaitu identifikasi area of concern dan skenario ancaman.

Tabel 5. *Area of Concern-Hardware*

No	***Areas of Concern***
1	Perangkat keras dapat diakses oleh pihak yang tidak berwenang jika tidak ada pengawasan fisik yang memadai. Ini berisiko terhadap potensi kebocoran data atau gangguan pada sistem yang sedang diintegrasikan.
2	Perangkat keras dapat mengalami kerusakan pada komponen seperti hard drive, RAM, atau prosesor yang berisiko menyebabkan hilangnya data penting yang digunakan dalam sistem integrasi.
3	Kurangnya pemeliharaan perangkat keras secara rutin dapat menurunkan kinerja sistem dan meningkatkan risiko kegagalan sistem integrasi yang dapat mempengaruhi operasional perusahaan.
4	Data yang disimpan pada perangkat keras harus dilindungi dengan baik untuk mencegah akses tidak sah, terutama ketika perangkat keras tersebut digunakan untuk mendukung proyek integrasi sistem yang melibatkan banyak pihak.
5	Router dan perangkat jaringan lainnya harus dikonfigurasi dengan benar untuk memastikan keamanan yang tepat, mencegah akses tidak sah, dan menjaga kestabilan jaringan yang digunakan dalam integrasi sistem antar perangkat.
6	Perangkat keras yang digunakan harus kompatibel dengan perangkat lunak dan sistem operasi yang digunakan oleh perusahaan untuk mendukung integrasi sistem yang lancar tanpa gangguan teknis.

Tabel 6. *Area of Concern-Software*

No	***Areas of Concern***
1	Perangkat lunak dapat terinfeksi oleh malware, virus, *trojan*, atau *ransomware* yang dapat merusak, mencuri, atau mengenkripsi data penting.
2	Cacat (*bug*) atau kerusakan pada kode perangkat lunak dapat menyebabkan data yang diproses menjadi tidak akurat (*corrupt*) atau bahkan hilang sepenuhnya.
3	Perangkat lunak memiliki performa yang buruk, seperti waktu pemuatan yang lama, *crash*, kegagalan server atau respons yang lambat bahkan tidak bisa diakses pengguna.
4	Perangkat lunak tidak kompatibel dengan sistem operasi, *hardware*, atau aplikasi lain, sehingga fungsinya tidak optimal atau bahkan tidak dapat berjalan.
5	Penggunaan perangkat lunak tanpa lisensi yang sah atau melanggar ketentuan lisensi yang berlaku.
6	Tidak adanya atau tidak berjalannya prosedur *backup* secara rutin, menyebabkan risiko kehilangan data
7	Risiko terkait pengelolaan dan penyimpanan data sensitif di *cloud*, termasuk kebutuhan untuk enkripsi data saat transit dan disimpan

Tabel 7. *Area of Concern*-Data dan Informasi

No	***Areas of Concern***
1	Risiko terkait pelanggaran privasi yang bisa berdampak negatif pada karyawan dan melanggar regulasi yang berlaku.
2	Risiko organisasi tidak mematuhi peraturan yang mengatur perlindungan data karyawan, yang dapat menyebabkan denda atau sanksi hukum.
3	Risiko terkait pemalsuan atau manipulasi data yang bisa merusak integritas laporan keuangan perusahaan.
4	Risiko yang dapat terjadi jika terjadi kegagalan pada sistem yang menyebabkan data keuangan yang penting tidak tersedia.
5	Risiko kebocoran informasi terkait desain perusahaan yang dapat menyebabkan hilangnya daya saing perusahaan.

Tabel 8. *Area of Concern*-Hak Akses dan Kredensial

No	***Areas of Concern***
1	Ancaman terkait dengan individu yang mendapatkan akses tanpa izin ke sistem atau data sensitif, baik oleh pihak internal maupun eksternal.
2	Penggunaan kata sandi yang lemah atau mudah ditebak, serta kurangnya kebijakan pengelolaan kredensial yang ketat, dapat memperbesar peluang akses tidak sah.
3	Serangan Berbasis Kredensial Misalnya serangan *brute-force*, *phishing*, atau pencurian kredensial yang dapat mengarah pada akses tidak sah ke sistem kritis.

Skenario ancaman dalam sistem informasi menggambarkan berbagai potensi risiko yang dapat mengganggu kerahasiaan, integritas, maupun ketersediaan data, perangkat keras, perangkat lunak, serta hak akses dan kredensial yang dimiliki perusahaan. Ancaman ini dapat berasal dari faktor internal, seperti kelalaian karyawan, penggunaan kata sandi yang lemah, atau kesalahan dalam pemeliharaan sistem, maupun dari faktor eksternal, seperti serangan malware, phishing, brute-force, hingga upaya peretasan yang menargetkan data sensitif dan infrastruktur penting. Motif yang melatarbelakangi ancaman bervariasi, mulai dari keuntungan finansial, sabotase, hingga lemahnya kesadaran keamanan di dalam organisasi. Dampak yang ditimbulkan pun signifikan, mencakup kebocoran data, kerugian finansial, gangguan operasional, hingga menurunnya reputasi perusahaan.

Fase IV: Identify and Mitigate Risk

Fase keempat bertujuan untuk mengidentifikasi serta merumuskan langkah mitigasi terhadap risiko yang telah dianalisis pada tahap sebelumnya. Pada tahap ini, organisasi menilai prioritas risiko berdasarkan tingkat kemungkinan (probability) dan dampaknya terhadap aset informasi yang kritis.

Tabel 9. Perhitungan Nilai Skor Relatif

Area Dampak (Nilai)	***Low (1)***	***Medium (2)***	***High (3)***
Reputasi & Kepercayaan (5)	5	10	15
Keuangan (4)	4	8	12
Produktivitas (3)	3	6	9
Denda dan Saksi Hukum (2)	2	4	6
Keselamatan dan Kesehatan (1)	1	2	3

Tabel tersebut didapatkan dari perhitungan:
Nilai Skor Relatif = Bobot Area Dampak × Severity (1–3)

Tabel 10. *Information Asset Risk - Hardware*

No	*Area of Concern*	*Information Asset Risk*		
1	Perangkat keras dapat diakses oleh pihak yang tidak berwenang jika tidak ada pengawasan fisik yang memadai. Ini berisiko terhadap potensi kebocoran data atau gangguan pada sistem yang sedang diintegrasikan.	***Consequences***		
		Insiden keamanan pada perangkat keras dapat menimbulkan berbagai konsekuensi serius, antara lain kerugian finansial akibat biaya perbaikan maupun pencurian aset, kebocoran data sensitif yang disalin atau diakses secara ilegal, hingga terganggunya operasional sistem karena perangkat yang rusak atau hilang tidak dapat digunakan lagi. Selain itu, insiden semacam ini juga berpotensi menurunkan tingkat kepercayaan pelanggan dan mitra bisnis terhadap perusahaan, yang pada akhirnya berdampak pada reputasi dan keberlangsungan operasional secara keseluruhan.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Medium*	4
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**41**
2	Perangkat keras dapat mengalami kerusakan pada komponen seperti hard drive, RAM, atau prosesor yang berisiko menyebabkan hilangnya data penting yang digunakan dalam sistem integrasi.	***Consequences***		
		Kehilangan data penting yang tersimpan dalam sistem integrasi dapat menimbulkan gangguan serius, mulai dari terhentinya layanan operasional karena server atau komputer tidak dapat berfungsi, hingga munculnya potensi downtime yang menghambat produktivitas perusahaan. Kondisi ini tidak hanya memengaruhi kelancaran proses bisnis sehari-hari, tetapi juga dapat berdampak pada efisiensi kerja secara keseluruhan.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*Medium*	10
		Keuangan	*High*	12
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Low*	2
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**34**
3	Kurangnya pemeliharaan perangkat keras secara rutin dapat menurunkan kinerja sistem dan meningkatkan risiko kegagalan sistem integrasi yang dapat mempengaruhi operasional perusahaan.	***Consequences***		
		Penurunan kinerja sistem dapat berdampak pada melambatnya proses operasional, sehingga aktivitas perusahaan tidak berjalan optimal. Selain itu, kegagalan perangkat keras seperti kerusakan pada hard drive, RAM, PSU, atau server berpotensi menyebabkan downtime yang menghambat kelancaran layanan serta mengganggu produktivitas secara keseluruhan.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*Medium*	10
		Keuangan	*High*	12
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Low*	2
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**34**
4	Data yang disimpan pada perangkat keras harus dilindungi dengan baik untuk	***Consequences***		
		Kebocoran atau perubahan data penting dapat menimbulkan konsekuensi serius bagi perusahaan, termasuk terjadinya pelanggaran		

	mencegah akses tidak sah, terutama ketika perangkat keras tersebut digunakan untuk mendukung proyek integrasi sistem yang melibatkan banyak pihak.	kerahasiaan informasi (*confidentiality breach*) yang mengancam keamanan dan integritas sistem. Dampak lain yang tidak kalah signifikan adalah menurunnya tingkat kepercayaan mitra dalam proyek integrasi, yang pada akhirnya dapat merugikan reputasi perusahaan dan menghambat kelancaran kerja sama strategis.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*Medium*	6
		Denda dan Saksi Hukum	*Medium*	4
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**38**
5	Router dan perangkat jaringan lainnya harus dikonfigurasi dengan benar untuk memastikan keamanan yang tepat, mencegah akses tidak sah, dan menjaga kestabilan jaringan yang digunakan dalam integrasi sistem antar perangkat.	***Consequences***		
		Gangguan pada kestabilan jaringan, baik berupa downtime maupun bottleneck, dapat berdampak pada terganggunya akses dan kelancaran layanan perusahaan. Kondisi ini tidak hanya menurunkan produktivitas, tetapi juga membuka peluang bagi ancaman yang lebih serius, seperti masuknya serangan malware atau ransomware, yang berpotensi memperparah kerusakan sistem serta meningkatkan risiko kebocoran maupun kehilangan data penting.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*Medium*	8
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Medium*	4
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**37**
6	Perangkat keras yang digunakan harus kompatibel dengan perangkat lunak dan sistem operasi yang digunakan oleh perusahaan untuk mendukung integrasi sistem yang lancar tanpa gangguan teknis.	***Consequences***		
		Gangguan teknis pada operasional dapat menyebabkan aplikasi tidak berfungsi secara optimal, sehingga sistem integrasi tidak berjalan sebagaimana mestinya. Kondisi ini berpotensi menimbulkan downtime yang menghambat aktivitas bisnis serta menunda penyelesaian proyek akibat perlunya proses troubleshooting tambahan, yang pada akhirnya dapat berdampak pada penurunan produktivitas dan efisiensi perusahaan.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*Medium*	10
		Keuangan	*High*	12
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Low*	2
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**34**

Tabel 11. *Information Asset Risk - Software*

No	***Area of Concern***	***Information Asset Risk***
1	Perangkat lunak dapat terinfeksi oleh malware, virus, trojan, atau ransomware yang dapat merusak, mencuri, atau mengenkripsi data penting.	***Consequences***
		Kehilangan atau kerusakan data dapat menimbulkan dampak yang serius bagi perusahaan, karena tidak hanya mengganggu kelancaran operasional akibat sistem yang lumpuh, tetapi juga berpotensi menurunkan reputasi perusahaan apabila kebocoran data sampai diketahui oleh pihak eksternal. Kondisi ini tidak hanya memengaruhi

		kepercayaan pelanggan dan mitra bisnis, tetapi juga dapat menimbulkan kerugian finansial serta meningkatkan risiko hukum bagi perusahaan.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Medium*	4
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**41**
2	Cacat (*bug*) atau kerusakan pada kode perangkat lunak dapat menyebabkan data yang diproses menjadi tidak akurat *(corrupt)* atau bahkan hilang sepenuhnya.	***Consequences***		
		Data yang diproses berisiko menjadi salah, rusak, atau corrupt sehingga tidak dapat digunakan kembali. Kondisi ini akan berdampak pada ketidakakuratan hasil analisis bisnis yang dihasilkan, sehingga keputusan yang diambil pun berpotensi keliru. Lebih jauh, jika kerusakan data terjadi secara permanen, perusahaan dapat kehilangan data penting yang berharga dan sulit dipulihkan, yang pada akhirnya memengaruhi keberlangsungan operasional dan efektivitas organisasi.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*Medium*	10
		Keuangan	*High*	12
		Produktivitas	*High*	10
		Denda dan Saksi Hukum	*Medium*	9
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**36**
3	Perangkat lunak memiliki performa yang buruk, seperti waktu pemuatan yang lama, crash, kegagalan server atau respons yang lambat bahkan tidak bisa diakses pengguna.	***Consequences***		
		Gangguan performa perangkat lunak dapat menimbulkan berbagai konsekuensi yang signifikan bagi operasional perusahaan. Waktu pemuatan aplikasi yang lama, crash, atau kegagalan server menyebabkan pengguna kesulitan mengakses layanan dan menghambat kelancaran pekerjaan sehari-hari. Kondisi ini berdampak langsung pada penurunan produktivitas serta potensi keterlambatan proyek akibat perlunya waktu tambahan untuk melakukan pemulihan sistem.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*Medium*	10
		Keuangan	*Medium*	8
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Low*	2
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**30**
4	Perangkat lunak tidak kompatibel dengan sistem operasi, hardware, atau aplikasi lain, sehingga fungsinya tidak optimal atau bahkan tidak dapat berjalan.	***Consequences***		
		Ketidakcocokan perangkat lunak dengan sistem operasi, perangkat keras, atau aplikasi lain dapat menyebabkan fungsi sistem tidak optimal atau bahkan tidak dapat berjalan sama sekali. Kondisi ini berpotensi menghambat integrasi sistem, menimbulkan downtime, dan mengurangi produktivitas. Selain itu, perusahaan dapat menanggung kerugian finansial akibat perlunya penyesuaian, pembelian lisensi baru, atau penggantian perangkat yang kompatibel.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*Medium*	10
		Keuangan	*High*	12
		Produktivitas	*High*	9

		Denda dan Saksi Hukum	*Low*	2
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**34**
5	Penggunaan perangkat lunak tanpa lisensi yang sah atau melanggar ketentuan lisensi yang berlaku.	***Consequences***		
		Penggunaan perangkat lunak tanpa lisensi resmi atau melanggar ketentuan lisensi dapat menimbulkan risiko serius bagi perusahaan. Selain ancaman hukum berupa denda dan sanksi dari regulator maupun pemilik hak cipta, kondisi ini juga dapat merugikan reputasi perusahaan karena dianggap tidak profesional dan tidak patuh terhadap regulasi.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*Medium*	6
		Denda dan Saksi Hukum	*High*	6
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**40**
6	Tidak adanya atau tidak berjalannya prosedur backup secara rutin, menyebabkan risiko kehilangan data	***Consequences***		
		Ketiadaan atau kegagalan prosedur backup rutin menimbulkan risiko serius berupa hilangnya data penting yang sulit atau bahkan tidak dapat dipulihkan. Kondisi ini dapat menyebabkan gangguan besar pada operasional perusahaan karena sistem tidak mampu memulihkan data setelah insiden, seperti kerusakan perangkat, serangan ransomware, atau human error. Dampaknya tidak hanya menghambat produktivitas dan menimbulkan kerugian finansial, tetapi juga dapat merusak reputasi perusahaan apabila data yang hilang berhubungan dengan pelanggan atau mitra bisnis.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Medium*	4
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**41**
7	Risiko terkait pengelolaan dan penyimpanan data sensitif di cloud, termasuk kebutuhan untuk enkripsi data saat transit dan disimpan	***Consequences***		
		Pengelolaan dan penyimpanan data sensitif di cloud tanpa perlindungan yang memadai, seperti enkripsi saat transit maupun saat disimpan, dapat menyebabkan kebocoran atau pencurian data. Insiden ini berpotensi menurunkan kepercayaan pelanggan dan mitra bisnis, menimbulkan kerugian finansial akibat kehilangan aset informasi yang berharga, serta dapat memicu sanksi hukum karena melanggar regulasi perlindungan data.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*Medium*	6
		Denda dan Saksi Hukum	*High*	6
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**40**

Tabel 12. *Information Asset Risk* - Data dan Informasi

No	*Area of Concern*	*Information Asset Risk*		
1	Risiko terkait pelanggaran privasi yang bisa berdampak negatif pada karyawan dan melanggar regulasi yang berlaku.	***Consequences***		
		Pelanggaran privasi individu dapat menimbulkan dampak serius bagi perusahaan karena tidak hanya melanggar hak personal, tetapi juga berpotensi melanggar hukum dan regulasi yang berlaku, seperti UU Perlindungan Data Pribadi atau GDPR. Situasi ini dapat mengakibatkan sanksi hukum maupun denda yang merugikan, serta menurunkan tingkat kepercayaan karyawan terhadap perusahaan. Jika tidak ditangani dengan baik, insiden tersebut dapat melemahkan citra organisasi sekaligus memengaruhi hubungan kerja dan produktivitas secara keseluruhan.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*Medium,*	6
		Denda dan Saksi Hukum	*High*	6
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**40**
2	Risiko organisasi tidak mematuhi peraturan yang mengatur perlindungan data karyawan, yang dapat menyebabkan denda atau sanksi hukum.	***Consequences***		
		Ketidakpatuhan organisasi terhadap peraturan perlindungan data karyawan dapat menimbulkan dampak hukum yang serius, mulai dari denda administratif hingga sanksi pidana sesuai regulasi yang berlaku, seperti UU PDP maupun GDPR. Insiden ini juga dapat menurunkan reputasi perusahaan di mata publik karena dianggap tidak memprioritaskan keamanan dan privasi data pribadi. Selain itu, keuangan perusahaan akan terdampak karena adanya potensi biaya denda dan pengeluaran tambahan untuk pemulihan kepatuhan.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*Medium*	6
		Denda dan Saksi Hukum	*High*	6
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**40**
3	Risiko terkait pemalsuan atau manipulasi data yang bisa merusak integritas laporan keuangan perusahaan.	***Consequences***		
		Pemalsuan atau manipulasi data laporan keuangan dapat merusak integritas perusahaan secara signifikan. Laporan keuangan yang tidak akurat akan menyesatkan pengambilan keputusan manajemen serta menurunkan tingkat kepercayaan investor, mitra, maupun regulator. Hal ini dapat memicu kerugian finansial besar, baik dalam bentuk hilangnya investasi maupun potensi sanksi hukum akibat pelanggaran standar akuntansi.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*Medium*	6
		Denda dan Saksi Hukum	*High*	6
		Keselamatan dan Kesehatan	*low*	1
		Relative Risk Score		**40**
4	Risiko yang dapat terjadi jika terjadi kegagalan pada sistem yang menyebabkan	***Consequences***		
		Kegagalan pada sistem yang mengelola data keuangan dapat menimbulkan dampak signifikan bagi perusahaan. Data keuangan yang		

	data keuangan yang penting tidak tersedia.	tidak tersedia akan menghambat aktivitas bisnis utama, termasuk pelaporan, transaksi, dan pengambilan keputusan strategis. Kondisi ini dapat menyebabkan keterlambatan dalam pemenuhan kewajiban finansial, menimbulkan potensi kerugian, serta merusak reputasi perusahaan di mata investor maupun mitra bisnis.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*Medium*	10
		Keuangan	*High*	12
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Medium*	4
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**36**
5	Risiko kebocoran informasi terkait desain perusahaan yang dapat menyebabkan hilangnya daya saing perusahaan.	***Consequences***		
		Kebocoran informasi yang berkaitan dengan desain perusahaan dapat mengakibatkan hilangnya daya saing strategis. Informasi teknis atau desain yang jatuh ke tangan pihak yang tidak berwenang, termasuk kompetitor, dapat dimanfaatkan untuk meniru, memodifikasi, atau bahkan mengungguli inovasi perusahaan. Hal ini akan menurunkan reputasi perusahaan sebagai pelaku bisnis yang inovatif, sekaligus menimbulkan kerugian finansial jangka panjang akibat hilangnya peluang pasar. Selain itu, kebocoran data intelektual juga dapat mengakibatkan potensi sengketa hukum terkait hak kekayaan intelektual dan melemahkan kepercayaan mitra bisnis.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	High	15
		Keuangan	High	12
		Produktivitas	Medium	6
		Denda dan Saksi Hukum	Medium	4
		Keselamatan dan Kesehatan	low	1
		Relative Risk Score		**38**

Tabel 13. *Information Asset Risk* - Hak Akses dan Kredensial

No	***Area of Concern***	***Information Asset Risk***		
1	Ancaman terkait dengan individu yang mendapatkan akses tanpa izin ke sistem atau data sensitif, baik oleh pihak internal maupun eksternal.	***Consequences***		
		Akses tidak sah ke sistem atau data sensitif dapat menimbulkan kebocoran informasi penting milik perusahaan maupun klien. Hal ini berpotensi merusak reputasi perusahaan karena hilangnya kepercayaan dari mitra bisnis dan pelanggan yang merasa dirugikan. Selain itu, insiden tersebut dapat mengakibatkan kerugian finansial signifikan, baik karena pencurian data maupun biaya pemulihan sistem, serta berpotensi memicu sanksi hukum akibat pelanggaran regulasi perlindungan data yang berlaku.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*Medium*	6
		Denda dan Saksi Hukum	*High*	
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**40**
2		***Consequences***		

	Penggunaan kata sandi yang lemah atau mudah ditebak, serta kurangnya kebijakan pengelolaan kredensial yang ketat, dapat memperbesar peluang akses tidak sah.	Penggunaan kata sandi yang lemah atau mudah ditebak, ditambah dengan ketiadaan kebijakan kredensial yang ketat, dapat membuka peluang besar bagi pihak tidak sah untuk memperoleh akses ke sistem. Jika hal ini terjadi, maka data sensitif perusahaan berisiko dicuri, dimodifikasi, atau bahkan dimusnahkan. Dampaknya mencakup kerugian finansial akibat insiden keamanan, menurunnya kepercayaan pelanggan maupun mitra bisnis, serta potensi sanksi hukum jika data yang dilindungi oleh regulasi ikut terdampak.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*Medium*	10
		Keuangan	*High*	12
		Produktivitas	*Medium*	6
		Denda dan Saksi Hukum	*Medium*	4
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**33**
3	Serangan Berbasis Kredensial Misalnya serangan brute-force, phishing, atau pencurian kredensial yang dapat mengarah pada akses tidak sah ke sistem kritis	***Consequences***		
		Serangan berbasis kredensial, seperti brute-force, phishing, atau pencurian kredensial, dapat memberikan akses tidak sah ke sistem kritis perusahaan. Jika berhasil, serangan ini berpotensi menyebabkan kebocoran data sensitif, kerugian finansial akibat pencurian maupun biaya pemulihan, serta gangguan operasional yang menghambat produktivitas. Lebih jauh, perusahaan bisa kehilangan kepercayaan pelanggan dan menghadapi sanksi hukum akibat pelanggaran regulasi keamanan data.		
		Severity		
		Impact Area	***Value***	***Score***
		Reputasi & Kepercayaan	*High*	15
		Keuangan	*High*	12
		Produktivitas	*High*	9
		Denda dan Saksi Hukum	*Medium*	4
		Keselamatan dan Kesehatan	*Low*	1
		Relative Risk Score		**41**

Tahapan terakhir dari fase ini adalah memilih pendekatan mitigasi yang akan menentukan semua risiko yang telah diidentifikasi berdasarkan relative risk score.

Penerapan pendekatan mitigasi memberikan dukungan yang signifikan dalam menentukan status rekomendasi atas setiap risiko yang telah diidentifikasi.

Tabel 14. *Risk Relative Matrix*

Risk Relative Matrix		
Risk Score	***POOL***	***Mitigation Approach***
30-45	1	Mitigasi (*Mitigate*)
16-29	2	Tunda (*Defer*)
0-15	3	Terima (Accept)

Tabel 15. Pemetaan Mitigasi

No	***Aset***	***Area of Concern***	***Risk Relative Matrix***	***POOL***	***Migration Approach***
1	*Hard ware*	Perangkat keras dapat diakses oleh pihak yang tidak berwenang jika tidak ada pengawasan fisik yang memadai. Ini berisiko terhadap potensi kebocoran data atau gangguan pada sistem yang sedang diintegrasikan.	41	1	Mitigasi
2	Hard ware	Perangkat keras dapat mengalami kerusakan pada komponen seperti hard drive, RAM, atau prosesor yang berisiko menyebabkan hilangnya data penting yang digunakan dalam sistem integrasi.	34	1	Mitigasi

3	Hard ware	Kurangnya pemeliharaan perangkat keras secara rutin dapat menurunkan kinerja sistem dan meningkatkan risiko kegagalan sistem integrasi yang dapat mempengaruhi operasional perusahaan.	34	1	Mitigasi
4	Hard ware	Data yang disimpan pada perangkat keras harus dilindungi dengan baik untuk mencegah akses tidak sah, terutama ketika perangkat keras tersebut digunakan untuk mendukung proyek integrasi sistem yang melibatkan banyak pihak.	38	1	Mitigasi
5	Hard ware	Router dan perangkat jaringan lainnya harus dikonfigurasi dengan benar untuk memastikan keamanan yang tepat, mencegah akses tidak sah, dan menjaga kestabilan jaringan yang digunakan dalam integrasi sistem antar perangkat.	37	1	Mitigasi
6	Hard ware	Perangkat keras yang digunakan harus kompatibel dengan perangkat lunak dan sistem operasi yang digunakan oleh perusahaan untuk mendukung integrasi sistem yang lancar tanpa gangguan teknis.	34	1	Mitigasi
7	Softw are	Perangkat lunak dapat terinfeksi oleh malware, virus, trojan, atau ransomware yang dapat merusak, mencuri, atau mengenkripsi data penting.	41	1	Mitigasi
8	Softw are	Cacat (bug) atau kerusakan pada kode perangkat lunak dapat menyebabkan data yang diproses menjadi tidak akurat (corrupt) atau bahkan hilang sepenuhnya.	36	1	Mitigasi
9	Softw are	Perangkat lunak memiliki performa yang buruk, seperti waktu pemuatan yang lama, crash, kegagalan server atau respons yang lambat bahkan tidak bisa diakses pengguna.	30	1	Mitigasi
10	Softw are	Perangkat lunak tidak kompatibel dengan sistem operasi, hardware, atau aplikasi lain, sehingga fungsinya tidak optimal atau bahkan tidak dapat berjalan.	34	1	Mitigasi
11	Softw are	Penggunaan perangkat lunak tanpa lisensi yang sah atau melanggar ketentuan lisensi yang berlaku.	40	1	Mitigasi
12	Softw are	Tidak adanya atau tidak berjalannya prosedur backup secara rutin, menyebabkan risiko kehilangan data	41	1	Mitigasi
13	Softw are	Risiko terkait pengelolaan dan penyimpanan data sensitif di cloud, termasuk kebutuhan untuk enkripsi data saat transit dan disimpan	40	1	Mitigasi
14	Data dan Infor masi	Risiko terkait pelanggaran privasi yang bisa berdampak negatif pada karyawan dan melanggar regulasi yang berlaku.	40	1	Mitigasi
15	Data dan Infor masi	Risiko organisasi tidak mematuhi peraturan yang mengatur Relative Risk Score 40 Consequences perlindungan data karyawan, yang dapat menyebabkan denda atau sanksi hukum.	40	1	Mitigasi
16	Data dan Infor masi	Risiko terkait pemalsuan atau manipulasi data yang bisa merusak integritas laporan keuangan perusahaan.	40	1	Mitigasi

17	Data dan Informasi	Risiko yang dapat terjadi jika terjadi kegagalan pada sistem yang menyebabkan data keuangan yang penting tidak tersedia.	36	1	Mitigasi
18	Data dan Informasi	Risiko kebocoran informasi terkait desain perusahaan yang dapat menyebabkan hilangnya daya saing perusahaan.	38	1	Mitigasi
19	Hak akses dan kredensial	Ancaman terkait dengan individu yang mendapatkan akses tanpa izin ke sistem atau data sensitif, baik oleh pihak internal maupun eksternal.	40	1	Mitigasi
20	Hak akses dan kredensial	Penggunaan kata sandi yang lemah atau mudah ditebak, serta kurangnya kebijakan pengelolaan kredensial yang ketat, dapat memperbesar peluang akses tidak sah.	33	1	Mitigasi
21	Hak akses dan kredensial	Serangan Berbasis Kredensial Misalnya serangan brute-force, phishing, atau pencurian kredensial yang dapat mengarah pada akses tidak sah ke sistem kritis	41	1	Mitigasi

Tabel 16. Rekomendasi Mitigasi

Aset	Rekomendasi Mitigasi
Hardware	Mitigasi Teknis - Menggunakan *server clustering* atau *failover system* agar layanan tetap berjalan walaupun terdapat server mengalami kegagalan. Mitigasi Prosedural - Terapkan jadwal penggantian perangkat sesuai siklus hidup (misalnya 3–5 tahun untuk server) dan memastikan adanya dukungan dari prinsipal. - Menyediakan anggaran khusus untuk pembaruan hardware secara berkala.
Software	Mitigasi Teknis: - Mengimplementasi *Endpoint Detection and Response* (EDR) untuk mendeteksi pola serangan atau ancaman. - Mengimplementasi *email security gateway* seperti *Microsoft Exchange Online Protection* untuk menyaring *phishing, spam*, dan lampiran berbahaya. - Menggunakan *network firewall & intrusion prevention system* (IPS) misalnya *Fortinet* untuk membatasi serangan dari jaringan. Mitigasi Prosedural - Lakukan pelatihan *cyber security awareness* rutin untuk karyawan. - Siapkan *Disaster Recovery Plan* (DRP) untuk aplikasi kritikal agar bisnis tetap berjalan saat terjadi gangguan.
Data dan Informasi	Mitigasi Teknis - Menerapkan *Data Loss Prevention* (DLP) untuk mencegah kebocoran data pribadi karyawan dan perusahaan. - Terapkan *Database Activity Monitoring* (DAM) untuk deteksi manipulasi dokumen. - Implementasi *backup* otomatis dengan enkripsi dan replikasi ke DRC. Mitigasi Prosedural - Membuat SOP akses data karyawan: siapa yang boleh membuka, berapa lama, dan untuk tujuan apa. - Terapkan *Non-Disclosure Agreement* (NDA) bagi pihak internal maupun eksternal. - Melakukan *awareness training* tentang pentingnya melindungi data perusahaan.
Hak akses dan kredensial	Mitigasi Teknis - Gunakan *Multi-Factor Authentication* (MFA) di semua akun pengguna - Terapkan *Zero Trust Access*: akses hanya berdasarkan identitas & kondisi perangkat. - Menerapkan *Account Lockout Policy* yaitu aturan untuk mengunci akun otomatis setelah gagal login beberapa kali (misalnya 5 kali).

	Mitigasi Prosedural - Menerapkan SOP perubahan kata sandi berkala. Seperti kebijakan rotasi sandi setiap 90 hari (atau lebih adaptif berdasarkan risiko) dan password lama tidak boleh digunakan ulang. - Membuat prosedur khusus jika ada indikasi ancaman hak akses seperti *brute force* atau *credential theft*. Dengan alur deteksi – notifikasi SOC – lock akun – reset password – investigasi log – laporan insiden.

KESIMPULAN

Metode OCTAVE Allegro terbukti relevan dan aplikatif untuk mengidentifikasi, menganalisis, dan memitigasi risiko TI dalam konteks perusahaan sistem integrator. Proses yang sistematis mulai dari identifikasi aset, ancaman, kerentanan, hingga dampak memberikan gambaran menyeluruh mengenai tingkat risiko yang dihadapi organisasi.

Terdapat empat aset utama dalam Teknologi Informasi (TI) yang dikelola oleh Perusahaan Sistem Integrator yakni Hardware, Software, Data dan Informasi, serta Hak akses dan kredensial. Keempat aset ini dianggap sebagai aset kritis karena memiliki peran yang vital untuk mendukung proses bisnis dan operasional perusahaan.

Berdasarkan matrix penilaian risiko, Data dan Informasi menjadi aset yang paling rentan. Hal ini ditunjukan dengan rata-rata skor tertinggi yakni 38,8. Hal ini berkaitan dengan potensi kehilangan data atau penyalahgunaan data yang akan berdampak luas mulai dari menurunnya tingkat kepercayaan pelanggan sehingga berdampak kerugian finansial yang tentunya mengganggu operasional dan produktivitas perusahaan. Aset lainnya juga mendapatkan skor dengan selisih yang sedikit. Untuk Hak Akses dan Kredensial dengan rata-rata skor 38. Software dengan rata-rata skor 37,42. Dan hardware dengan rata-rata skor 36,33. Hal ini menandakan seluruh aset perlu dikelola dengan baik untuk mencegah dan meminimalisasi gangguan dalam penggunaan Teknologi Informasi

Seluruh area yang menjadi perhatian dalam penilaian risiko mengklasifikasikan berada pada POOL 1 yang menandakan secara mitigasi perlu segera dimulai. Keputusan terkait mitigasi risiko harus didasarkan pada pemahaman yang mendalam mengenai kemampuan dan prioritas perusahaan dalam mengelola dan mengurangi dampak risiko yang diidentifikasi.

Secara keseluruhan, penelitian ini menyimpulkan bahwa OCTAVE Allegro efektif sebagai kerangka kerja manajemen risiko TI. Dengan penerapan yang konsisten, perusahaan sistem integrator dapat meningkatkan ketahanan dan daya saingnya dalam menghadapi tantangan keamanan informasi yang semakin kompleks.

Hasil analisis risiko pada penelitian ini masih bersifat kontekstual dan terbatas pada perusahaan Sistem Integrator dan sangat bergantung pada persepsi responden sehingga terdapat potensi bias subjektif dalam menentukan prioritas dampak maupun level risiko. Untuk penelitian selanjutnya disarankan untuk melakukan kombinasi metode OCTAVE Allegro dengan kerangka lain seperti ISO 270001 atau NIST SP 800-30 agar analisis risiko secara teknis lebih komprehensif.

DAFTAR PUSTAKA

Abdullah, N., Hanafi, H., & Nawang, N. I. (2021). Digital Era and Intellectual Property Challenges in Malaysia. *Pertanika Journal Social Sciences & Humanities*, 205-219.

Asrin, F., Ismarmiaty, Putra, S. A., Setyoningrum, N. G., & dkk. (2024). *Keamanan Sistem Informasi.* Sleman, Yogyakarta: PT Penamudamedia.

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). *Introducing OCTAVE Allegro.* Pennsylvania, United States: Carnegie Mellon University.

Dewanto, N. (2025). *Gajah Tidur yang Terbangun : 50 Tahun Inovasi Digital Metrodata.* Jakarta: PT Kompas Media Nusantara.

Emmanuel, P., & Maulany, R. (2023). Penilaian Risiko Sistem Informasi Menggunakan Metode OCTAVE Allegro pada Indonesia Publishing House. *KREA-TIF: Jurnal Teknik Informatika*. https://doi.org/10.32832/krea-tif.v11i1.14179

Fathullah, M. A., & Subbarao, A. (2022). Security Risk Analysis for Information Asset. *Journal of System and Management Sciences, Vol. 12*. doi:10.33168/JSMS.2022.0412

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2022). Cybersecurity Risk Review of Financial Studies, Forthcoming. *Swiss Finance Institute Research*. https://doi.org/10.2139/ssrn.3725130

Harahap, A., Andani, C., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen dan Pemasaran Digital*. https://doi.org//10-38035/jmpd.v1.i2

Hom, J., Anong, B., Rii, K., Choi, L., & Zelina, K. (2020). The Octave Allegro Method in Risk Management Assessment of Educational

Institutions. *Aptisi Transactions on Technopreneurship (ATT)*.

Kristiana, R., Rochman, A. S., Yusuf, M., & etc. (2022). *Manajemen Risiko.* Sumedang, Jawa Barat: CV. Mega Press Nusantara.

Pardosi, V., Deta, B., Nugroho, F., & Vandika, A. (2024). *Sistem Keamanan Informasi.* Solok, Sumatera Barat: PT Mafy Media Literasi Indonesia.

Pelatta, T., Maelissa, N., Titaley, H., & Tuanakotta, A. (2023). Analisa Risiko Pada Proyek Pembangunan Gedung Auditorium IAIN Kota Ambon. *Journal Agregate, Vol 2 No.1*.

Prasetyaningrum, G., Nurmayanti, F., & Azahra, F. (2022). Faktor-Faktor Yang Mempengaruhi Etika Sistem Informasi: Moral, Isu Sosial Dan Etika Masyarakat(Literature Review Sim). *Jurnal Manajemen Pendidikan dan Ilmu Sosial, Vol. 3 No. 2*. https://doi.org/10.38035/jmpis.v3i2.1115

Rohman, A., Ambarwati, A., & Setiawan, E. (2020). Analisis Manajemen Risiko IT dan Keamanan Aset Menggunakan Metode Octave-S. *INTECOMS: Journal of Information Technology and Computer Science*. https://doi.org/10.31539/intecoms.v3i2.1854

Sarjana, S., Nardo, R., Hartono, R., Siregar, Z., Irmal, Sohilauw, M., Badrianto, Y. (2020). *Manajemen Risiko.* Bandung: CV Media Sains Indonesia.

Sopian, A. (2021). Pemanfaatan Teknologi Informasi dan Digital pada Pendidikan Dasar Islam di MI Islam Tonoboyo Magelang. *Journal of Primary Education, Vol 1 No 2*. https://doi.org/10.37680/basica.v1i2.1039

Suryawijaya, T. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*. https://doi.org/10.21787/jskp.2.2023.55-68

Syafii, I., & Siregar, S. (2020). Manajemen Risiko Perbankan Syariah. *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*, 662-665.