Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v12i2

Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro

B S Deva[1], **R Jayadi**[2]
Program Studi Manajemen Sistem Informasi, Universitas Bina Nusantara[12]
Jl. Kebon Jeruk Raya No. 27, Kebon Jeruk , Jakarta Barat, 11530, Indonesia[12]
bara.suradeva@binus.ac.id*[1], riyanto.jayadi@binus.edu[2]

diterima: 4 April 2022
direvisi: 10 Juni 2022
dipublikasi: 1 September 2022

Abstrak

PT. XYZ sebagai salah satu perusahaan yang bergerak di bidang *System Integrator* telah menggunakan teknologi informasi dalam menjalankan aktivitas bisnisnya. PT. XYZ merupakan penyedia solusi teknologi informasi dan komunikasi di Indonesia yang menyediakan layanan pengadaan & implementasi infrastruktur TI serta layanan keamanan teknologi informasi. Aset informasi yang dimiliki PT. XYZ adalah aset informasi internal perusahaan termasuk aset informasi terkait *customer.* Sehingga dibutuhkan manajemen sistem informasi yang handal dan mendukung prinsip keamanan informasi yaitu kerahasiaan, keutuhan, dan ketersediaan. Pada tahun 2019 PT. XYZ mengalami insiden serangan *ransomware* yang mengakibatkan data – data proyek dan data *customer* ter-enkripsi. Hal ini berdampak terhadap produktivitas & reputasi perusahaan karena kehilangan aset informasi yang diperlukan. Dengan demikian diperlukan penilaian risiko untuk dapat menentukan strategi mitigasi risiko sebagai langkah manajemen risiko dalam mengatasi dan meminimalisir dampak permasalahan terkait keamanan informasi. Metode penilaian risiko yang digunakan dalam penelitian ini adalah Metode OCTAVE Allegro yang menggunakan 8 tahapan untuk dapat mengidentifikasi, menganalisa dan menentukan pendekatan mitigasi risiko. Penelitian ini mengidentifikasi aset informasi perusahaan berdasarkan pengumpulan data melalui wawancara narasumber PT.XYZ dan observasi. Dengan metode OCTAVE Allegro ditemukan 6 *area of concern* yang berpotensi menjadi risiko keamanan informasi dimana aset informasi teridentifikasi memiliki skor risiko relative ≥ 30 yang termasuk tinggi dalam rentang skor matriks risiko. Dengan demikian, diperlukan penilaian risiko untuk dapat menentukan strategi mitigasi risiko.

Kata kunci: Analisis Risiko; Sistem Keamanan Informasi; Mitigasi Risiko; OCTAVE Allegro; Aset Informasi

Abstract

PT. XYZ as a company engaged in the System Integrator has used information technology in carrying out its business activities. PT. XYZ is a provider of information and communication technology solutions in Indonesia that provides IT infrastructure procurement & implementation services as well as information technology security services. Information assets owned by PT. XYZ is the company's internal information assets including customer-related information assets. So that a reliable information system management is needed that supports the principles of information security, namely confidentiality, integrity, and availability. In 2019 PT. XYZ experienced a ransomware attack incident that resulted in encrypted project data and customer data. This has an impact on the productivity & reputation of the company due to the loss of necessary information assets. Thus an assessment is needed to be able to determine a mitigation strategy as a management step in overcoming and reducing the impact of problems related to information. The assessment method used in this study is the OCTAVE Allegro method which uses 8 stages to identify, analyze and determine risk mitigation approaches. This study identifies company information assets based on data collection through interviews with PT.XYZ sources and

observations. With the OCTAVE Allegro 6 area of concern method that may be at risk of information security risk, information assets have a relative risk score of ≥ 30 which is included in the risk risk range. Thus, consideration is needed to be able to determine risk mitigation strategies.
Keywords: *Risk Analysis; Information Security; Risk Mitigation; OCTAVE Allegro; Information Asset*

1. Pendahuluan

Pemanfaatan teknologi informasi pada perusahaan saat ini telah menjadi kebutuhan penting yang berperan dalam mendukung aktivitas bisnis. Peran teknologi informasi pada perusahaan menjadikan data sebagai aset informasi yang sangat bernilai bagi kelangsungan bisnis karena dapat membantu perusahaan dalam melakukan pengambilan keputusan, mengelola aset informasi, mengakses informasi dan juga berbagi informasi secara cepat, mudah, efektif dan efisien. PT. XYZ sebagai perusahaan yang bergerak di bidang System Integrator telah menggunakan teknologi informasi dalam menjalankan kegiatan usahanya. PT. XYZ adalah penyedia solusi teknologi informasi dan komunikasi di Indonesia yang menyediakan layanan pengadaan & implementasi infrastruktur TI serta layanan keamanan teknologi informasi. Informasi aset yang dimiliki oleh PT. XYZ merupakan aset informasi internal perusahaan termasuk aset informasi yang berhubungan dengan pelanggan.

Pada tahun 2019 PT. XYZ mengalami insiden serangan *ransomware* yang mengakibatkan data proyek dan data pelanggan terenkripsi. Serangan ini mengakibatkan aset informasi perusahaan yang terkena *ransomware* tidak dapat dipulihkan sebelum PT. XYZ membayar jumlah yang diminta oleh pembuat atau pengirim *ransomware*. Pemulihan data alternatif melalui cadangan data yang disimpan tidak dapat dipulihkan atau mengembalikan data secara utuh karena ada aset informasi yang belum dibackup akibat kelalaian pegawai. Hal ini berdampak pada produktivitas & reputasi perusahaan karena hilangnya aset informasi yang diperlukan. Ada juga *malware* yang terdeteksi oleh fitur keamanan *Endpoint Security* yang terpasang di laptop karyawan yang menunjukkan cukup banyak file atau data yang berpotensi *malware*. Potensi infeksi *malware* dapat terjadi ketika karyawan tidak sadar saat mendownload file atau aplikasi yang ternyata telah disisipkan malware sehingga berpotensi menginfeksi data bahkan perangkat lain yang dapat mengancam keamanan informasi dari suatu data. Dengan demikian, diperlukan penilaian risiko untuk dapat menentukan strategi mitigasi risiko sebagai langkah manajemen risiko dalam mengatasi dan meminimalkan dampak permasalahan terkait keamanan informasi.

Metode penilaian risiko yang digunakan dalam penelitian ini adalah Metode OCTAVE Allegro. Metode ini mampu berfokus terhadap penilaian risiko aset informasi sesuai dengan cakupan yang dibutuhkan perusahaan. Metode penilaian risiko yang digunakan dalam penelitian ini adalah metode OCTAVE Allegro. Metode ini berfokus pada penilaian risiko aset informasi di bawah ruang lingkup yang dibutuhkan oleh perusahaan. Berdasarkan penelitian terdahulu yang telah dilakukan, terdapat beberapa contoh kasus terkait analisa risiko & keamanan informasi dengan menggunakan metode OCTAVE Allegro. Berikut merupakan referensi studi kasus terkait penggunaan metode OCTAVE Allegro:

1. Penggunaan metode OCTAVE Allegro untuk memfokuskan penilaian pada aset informasi dan relatif mudah digunakan karena perusahaan tidak membutuhkan banyak sumber daya untuk menggunakannya sehingga cocok untuk diaplikasikan di perusahaan kecil dan menengah seperti PT ABC. Sistem pelayanan publik PT ABC dipilih sebagai objek kasus penelitian karena sebelumnya tidak dilakukan penilaian risiko [1].
2. Penelitian terhadap situs *Schoology.com* yang mengklaim telah memiliki jutaan pengguna. Penelitian ini membahas tentang penerapan penilaian risiko pada sistem informasi dengan menggunakan pendekatan OCTAVE Allegro terhadap potensi

ancaman yang mungkin terjadi pada situs *Schoology.com.* Metode OCTAVE Allegro dipilih, karena dianggap *agile* fleksibel, dan telah terbukti bahwa metode penilaian risiko dengan menggunakan OCTAVE Allegro memiliki kemampuan untuk memberikan hasil yang baik, dengan investasi yang relatif kecil dalam hal waktu dan sumber daya, bahkan untuk organisasi yang tidak memiliki keahlian manajemen risiko yang baik [2].

3. Penelitian yang dilakukan oleh di perusahaan yang mengoperasikan sistem E-Money. Penelitian menggunakan metode OCTAVE Allegro untuk membuat penilaian risiko yang bertujuan untuk membantu perusahaan memilih sebelum mengetahui jenis risiko yang akan terjadi. untuk mengidentifikasi dan mengevaluasi risiko keamanan informasi [3].

Pada kasus penelitian ini, penulis bertujuan untuk dapat melakukan penilaian risiko dengan metode OCTAVE Allegro yang kemudian dapat mendukung strategi mitigasi yang tepat serta mengetahui kelebihan dan kekurangan dari penggunaan metode ini. PT. XYZ belum pernah melakukan penilaian risiko dan juga tidak memiliki sumber daya yang berpengalaman dalam melakukan penilaian risiko. Namun demikian metode OCTAVE Allegro dapat diterapkan dan dilakukan oleh individu pemula mengenai penilaian risiko dalam implementasinya. Metode OCTAVE Allegro memiliki pendekatan yang paling tepat untuk kebutuhan penilaian risiko keamanan informasi yang dapat mendukung strategi mitigasi sesuai dengan risiko ancamannya

2. Kajian Pustaka

2.1 Risiko

Risiko adalah kemungkinan suatu peristiwa mengalami kerugian ekonomi dan finansial atau kerusakan material fisik, sebagai akibat dari ketidakpastian yang terkait dengan tindakan yang diambil [4]. Dasar pengukuran risiko yang dikemukakan oleh Bernoulli adalah pengukuran risiko menggunakan geometri untuk meminimalkan penyebaran risiko berdasarkan rangkaian kejadian dimana risiko diukur dengan menggunakan dua variabel gabungan yaitu frekuensi kejadian risiko dan tingkat konsekuensi dari suatu kejadian [5].

2.2 Keamanan Informasi

Keamanan informasi dapat didefinisikan sebagai “perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi serta elemen-elemen kritisnya, termasuk perangkat lunak dan perangkat keras yang menggunakan, menyimpan, memproses, dan mengirimkan informasi tersebut melalui penerapan teknologi, pendidikan, dan kesadaran [6]. Tujuan Keamanan Informasi adalah untuk memastikan: kerahasiaan, integritas, ketersediaan dan akuntabilitas sumber daya yang menjadi tanggung jawab organisasi [7]. Di area *cloud computing*, desain dan implementasi kontrol keamanan informasi yang perlu diperhatikan oleh organisasi atau perusahaan adalah sebagai berikut [8]:

1. Jenis serangan dan dampak serangan
2. Mempertimbangkan tindakan pencegahan yang terkait dengan keamanan informasi
3. Mempertimbangkan risiko keamanan informasi
4. Mempelajari insiden penyerangan

Keamanan informasi dalam organisasi berusaha menganalisis strategi terbaik untuk melindungi aset informasi organisasi dari peretas. Jadi departemen keamanan TI perlu mengedukasi setiap karyawan dalam organisasi untuk meminimalkan celah keamanan. Sebagian besar pegawai tidak mengetahui atau kurang mengetahui masalah keamanan informasi sehingga diperlukan pedoman yang merupakan kebijakan keamanan informasi [9].

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v12i2

2.3 Ancaman Keamanan Informasi

Terdapat beberapa modus serangan terhadap sistem keamanan informasi yang sering terjadi di masa pandemi COVID-19. Berikut ini adalah jenis-jenis serangan [10]:

1. *Email phising*
2. Pesan SMS/WhatsApp
3. *Remote access* BYOD
4. *Remote acces* terhadap infrastruktur IT
5. Alat kesehatan
6. Aplikasi *mobile* COVID -19

Pelaku serangan siber memanfaatkan *email ransomware* dan *phishing* yang dirancang agar tampak seperti informasi yang berasal dari sumber tepercaya. Sehingga perlunya kewaspadaan pengguna saat mengklik link, membuka lampiran email, mengunduh *file* dan menginstal aplikasi [11].

2.5 Manajemen Risiko Keamanan Informasi

Pada dasarnya keamanan tidak hanya berupa keamanan data atau informasi, tetapi juga terdiri dari hal-hal fisik seperti: lokasi, orang dan keamanan lingkungan eksternal seperti cuaca. Sehingga sistem informasi tersebut membutuhkan suatu manajemen keamanan. Tujuannya adalah [12]:

1. Prioritas Keamanan
2. Tingkat Prioritas Keparahan
3. Menentukan Kontrol Keamanan yang Efektif
4. Melakukan Pengawasan Dan Evaluasi Manajemen Risiko

2.6 Analisis Risiko

Dalam operasional dan implementasi teknologi informasi, berbagai risiko dapat muncul yang dapat mengancam keberlangsungan proses bisnis sehingga diperlukan analisis risiko keamanan sistem informasi. Analisis risiko merupakan proses dasar dari keamanan informasi dan manajemen risiko. Analisis risiko adalah proses untuk memahami risiko dan menentukan tingkat risiko. Hasil analisis risiko menjadi dasar pengambilan keputusan untuk mengevaluasi risiko. Analisis risiko menggambarkan besarnya risiko berdasarkan konsekuensi dan kemungkinan terjadi [13]. Salah satu metode analisis risiko yang sesuai dengan kebutuhan perusahaan terkait penilaian risiko operasional teknologi informasi untuk dapat diimplementasikan adalah metode OCTAVE Allegro. Dengan metode OCTAVE Allegro dapat membantu menentukan strategi mitigasi risiko yang dibutuhkan perusahaan.

3. Metode Penelitian

3.1 Pengumpulan Data

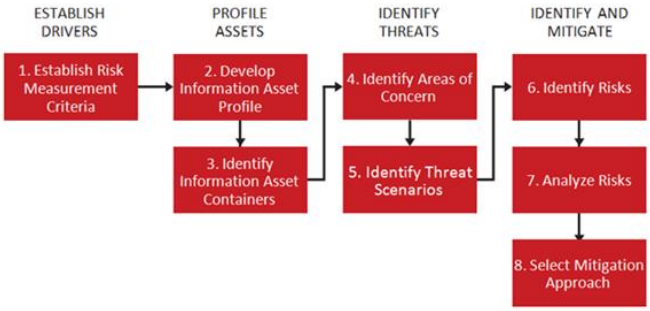
Pengumpulan data primer dilakukan secara langsung terhadap obyek penelitian yang sesuai. Metode pengumpulan data dilakukan dengan metode wawancara dan observasi. Pengumpulan data dilakukan dengan wawancara terhadap narasumber manajemen dan pimpinan PT. XYZ secara bergantian dengan memberikan beberapa pertanyaan yang diperlukan dalam melakukan penilaian risiko dengan menggunakan metode OCTAVE Allegro. Pengumpulan data secara observasi dilakukan dengan cara mengamati aktivitas operasional yang berhubungan dengan risiko keamanan aset informasi secara langsung di PT. XYZ. Observasi juga dilakukan pada aplikasi portal PT. XYZ, *local sharing folder* PT. XYZ, email termasuk *cloud* sebagai media penyimpanan aset informasi dan distribusi aset informasi PT.XYZ. Observasi terkait dengan aset informasi yaitu dokumen, *file* yang

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v12i2

bernilai penting bagi aktivitas bisnis PT.XYZ menjadi bahan penelitian sebagai pengumpulan data.

3.2 OCTAVE Allegro

Metode OCTAVE Allegro dikembangkan untuk memungkinkan berbagai penilaian risiko operasional organisasi yang mampu menghasilkan penilaian risiko yang efektif, andal, dan non-individu dengan pengetahuan penilaian risiko yang luas. Pendekatan metode OCTAVE Allegro melakukan penilaian risiko dengan fokus utama pada aset informasi dalam konteks bagaimana aset informasi tersebut digunakan, disimpan, didistribusikan, diproses, dan bagaimana aset informasi memiliki potensi ancaman, kerentanan, dan gangguan [14].



Gambar 1. Fase dan Tahapan metode OCTAVE Allegro

Metode yang digunakan dalam penulisan ini adalah metode OCTAVE Allegro. Metode OCTAVE Allegro terdiri dari delapan tahapan yang dikelompokkan ke dalam empat kategori atau fase seperti pada gambar 1. Keempat kategori tersebut adalah sebagai berikut:

1. Fase 1, tahap "*Define Drivers or Guidelines*" bertujuan untuk menentukan prioritas kriteria pengukuran risiko
2. Fase 2, langkah "*Profile Aset*" dirancang untuk mengidentifikasi dan mendokumentasikan aset logis, teknis, fisik, dan individual
3. Fase 3, langkah "*Identify Threats*" berfokus pada identifikasi ancaman terhadap aset yang diidentifikasi
4. Fase 4, langkah "*Identify & Mitigate*" melakukan identifikasi risiko sesuai dengan metode OCTAVE Allegro untuk aset informasi penting. Sehingga mampu menentukan strategi mitigasi yang sesuai dengan identifikasi dan penilaian risiko yang telah dilakukan

Keuntungan dari metodologi ini adalah bahwa metodologi ini sangat berfokus pada pengumpulan kebutuhan bisnis dan menyesuaikan penilaian risiko sesuai dengan kebutuhan prioritas. Metode OCTAVE Allegro dipilih, karena dianggap *agile*, fleksibel, dan telah terbukti bahwa metode penilaian risiko dengan menggunakan OCTAVE Allegro memiliki kemampuan untuk memberikan hasil yang baik, dengan investasi yang relatif kecil dalam hal waktu dan sumber daya, bahkan untuk organisasi yang tidak memiliki keahlian manajemen risiko yang baik OCTAVE Allegro melangkah lebih jauh dengan menyediakan kerangka dokumentasi referensi dalam bentuk lembar kerja untuk membantu penggunaan metodologi.

Penerapan metode analisis risiko OCTAVE Allegro PT. XYZ menggunakan seperangkat standar lembar kerja Allegro yang mendukung kesesuaian kerangka metode menurut setiap fase & tahapan [15]. Berikut ini adalah lembar (*worksheet*) kerja kategori fase Allegro 4 OCTAVE yang digunakan:

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v12i2

1. *Risk Measurement Criteria and Impact Area Priority*
2. *Critical Information Asset Profile*
3. *Critical Information Asset Profile*
4. *Asset Risk Information*

4. Hasil dan Pembahasan

4.1 Tahap 1. Define Drivers or Guidelines: Menetapkan Kriteria Pengukuran Risiko

Tahap ini dimulai dengan identifikasi area berdampak (*impact area*) PT. XYZ terkait dengan risiko ancaman keamanan informasi yang dapat digunakan sebagai pengukuran kriteria risiko dengan melakukan wawancara dengan pihak terkait untuk mengidentifikasi informasi perusahaan. Tabel 1 menunjukkan kriteria pengukuran risiko digunakan untuk mengukur dampak risiko pada *impact area*. Setelah informasi tentang *impact area* teridentifikasi, maka perlu memprioritaskan kriteria yang telah ditentukan. Prioritas ini menentukan nilai impact area perusahaan dari prioritas tertinggi hingga prioritas terendah.

Tabel 1. Kriteria Risiko dari Area Berdampak

Priority	*Impact Areas*
4	Reputasi dan kepercayaan customer
1	Finansial
3	Produktivitas
2	Keamanan dan Kesehatan
5	Denda dan Sanksi Hukum

4.2 Tahap 2. Profile Asset: Menyusun Profil Aset Informasi

Ada tujuh aset informasi penting & rahasia PT. XYZ diidentifikasi berdasarkan hasil pengumpulan data dengan wawancara dan observasi:

1. Perusahaan
2. *Customer*
3. Proyek
4. Karyawan
5. Keahlian
6. Infrastruktur TI
7. *Warehouse*

Tahapan ini membuat profil aset informasi PT. XYZ dan memilih informasi terdokumentasi sesuai dengan format yang disediakan oleh OCTAVE Allegro seperti pada tabel 2.

Tabel 2. *Critical Information Asset Profile*

Critical Information Asset Profile		
Critical Asset	*Rationale for Selection*	*Description*
Data Proyek	Kebocoran data proyek dan ancaman ketersediaan data dapat merusak reputasi & kepercayaan *customer* dan dapat berujung sanksi hukum terkait kerahasiaan data serta menggangu produktivitas.	Data Proyek mencakup informasi proyek dengan *customer,* dokumentasi laporan proyek, Laporan Managed Services SOC *Customer,* Laporan Pentest *Customer* informasi status proyek, BAST, laporan insiden proyek, status *service management.*

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v12i2

Owner(s)		
Head of Program Project & Services Management, Head of Professional Services		
Security Requirements		
Confidentiality	Hanya personel PT. XYZ yang memiliki otorisasi dapat mengakses aset informasi ini.	
Integrity	Hanya personel PT. XYZ yang memiliki otorisasi dapat mengubah aset informasi ini.	
Availability	Aset ini harus tersedia untuk dapat diakses kapanpun oleh personel PT. XYZ yang memiliki otorisasi.	
Most Important Security Requirement		
✓ *Confidentiality*	❑ *Integrity*	❑ *Availability*

4.3 Tahap 3. Profile Asset: Identifikasi Container Aset Informasi

Pada tahap ini dilakukan identifikasi setiap *container* aset informasi yang merupakan fokus dari detail tahapan dalam menentukan lembar kerja *information asset risk environment map*. *Container* adalah istilah di mana aset informasi disimpan. *Container* termasuk:

1. *Technical Container* (Perangkat Lunak, Perangkat Keras, Server, Perangkat Jaringan)
2. *Physical Container* (barang dalam bentuk fisik seperti file)
3. *People Container* (pemilik aset informasi baik dengan pihak internal atau eksternal)

Berdasarkan identifikasi pengumpulan data dengan wawancara dan observasi, penulis mengidentifikasi *container* teknis, fisik dan orang dari 7 aset informasi PT. XYZ yang masing-masing ditunjukkan pada tabel 3, 4, dan 5.

Tabel 3. *Information Asset Risk Environment Map Technical Container*

Internal	
Container Description	*Owner(s)*
Aplikasi portal PT. XYZ: berfungsi sebagai media untuk mengakses & menyimpan data.	PT. XYZ
Local Network Folder/File Sharing: berfungsi sebagai media penyimpanan data, mengakses data, berbagi atau transfer data.	PT. XYZ
Laptop/PC: Sebagai perangkat yang mendukung pekerjaan dalam mengolah, menyimpan dan mendistribusikan data dalam menjalankan aktivitas bisnis.	PT. XYZ
Outlook: berfungsi untuk mengirim dan menerima pesan termasuk dengan lampiran file yang berisi data.	PT. XYZ
VPN: Berfungsi untuk mengakses data pada local network folder/file sharing dengan terhubung di jaringan intranet pada saat melakukan *remote access.*	PT. XYZ
Server: melayani permintaan data & mengatur hak akses ke dalam jaringan terhadap *user.*	PT. XYZ
External	
Container Description	*Owner(s)*
Google Drive: berfungsi sebagai media penyimpanan data, mengakses data, & berbagi data.	Google
Dropbox: berfungsi sebagai media penyimpanan data, mengakses data, & berbagi data.	Dropbox

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v12i2

Pada tabel 3 yang merupakan *Information Asset Risk Environment Map* dari *technical container* menjelaskan melalui media apa saja aset informasi berupa data atau file PT.XYZ dapat diakses, dikelola dan dibagikan. Pihak *internal* dan *external* yang tertulis pada tabel 3 merupakan pemilik dari media pengelola aset informasi seperti *software*, *hardware*, maupun jaringan.

Tabel 4. *Information Asset Risk Environment Map Physical Container*

Internal	
Container Description	*Owner(s)*
Akta perusahaan	PT. XYZ
Laporan keuangan	PT.XYZ
Internal	
Container Description	*Owner(s)*
Laporan Keuangan	Auditor eksternal, PT. XYZ.

Pada tabel 4 yang merupakan *Information Asset Risk Environment Map* dari *physical container* menjelaskan bentuk fisik dari aset informasi berupa data atau file PT.XYZ. Pihak *internal* dan *external* yang tertulis pada tabel 4 merupakan pemilik dari aset informasi.

Tabel 5. *Information Asset Risk Environent Map People Container*

Internal Personnel	
Role/Responsibility	*Department or Unit*
Akta Perusahaan: *staff finance, Head of Finance,*	*Finance*
Laporan Keuangan: *staf finance, Head of Finance*	*Finance*
External Personnel	
Contractor, Vendor, etc	*Organization*
Laporan Keuangan: Tim auditor eksternal	PT.ABC

Pada tabel 5 yang merupakan *Information Asset Risk Environment Map* dari *people container* mengidentifikasi personel departemen atau unit yang memiliki aset informasi berupa data atau file PT.XYZ. Pihak *internal* dan *external* yang tertulis pada tabel 5 mengidentifikasi personel internal perusahaan atau eksternal perusahaan dari aset informasi.

4.4 Tahap 4. Identify Threat: Identifikasi Area Perhatian

Pada tahap ini, identifikasi area yang menjadi perhatian dan skenario ancaman dilakukan. Berdasarkan hasil wawancara dan observasi pengumpulan data teridentifikasi lima *area of concern* pada tabel 6 teridentifikasi *area of concern*.

Tabel 6. *Area of Concern* Teridentifikasi

No.	*Area of Concern*
1	Pengungkapan atau penyebaran data informasi sensitif secara tidak sah.
2	*Server Down*
3	Serangan *Ransomware*
4	Serangan *Malware*
5	Kerusakan *devices*
6	*Awareness* terkait keamanan informasi

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v12i2

Berdasarkan area yang menjadi perhatian, dilakukan analisis penilaian skenario ancaman, risiko, probabilitas kejadian, dan tingkat keparahan menggunakan lembar kerja Allegro *Information Assets Risk Environment Maps.*

4.5 Tahap 5. Identify Threat: Identifikasi Skenario Ancaman

Tahap 5 adalah mengidentifikasi area yang menjadi perhatian yang ditambahkan ke skenario ancaman. Yang perlu dilakukan adalah melengkapi tabel risiko aset informasi untuk mengidentifikasi setiap skenario ancaman. Berdasarkan *area of concern*, analisis penilaian dilakukan berdasarkan *area of concern*, skenario ancaman, risiko, probabilitas kejadian, dan tingkat keparahan menggunakan lembar kerja *Allegro Information Assets Risk Environment Maps.*

4.6 Tahap 6 & 7. Identify & Mitigate: Identifikasi & Analisis Risiko

Langkah selanjutnya adalah tahap terakhir, yaitu menentukan rekomendasi strategi mitigasi menggunakan lembar kerja mitigasi risiko Allegro pada tabel 7. Pada tahap ini, skor risiko relatif adalah diperhitungkan untuk menganalisis risiko dan membantu organisasi menentukan strategi risiko yang tepat. Berikut langkah-langkah untuk menghitung skor risiko relatif:

1. Mengkalikan nilai prioritas kriteria risiko pada kolom area dampak yang telah ditentukan pada tahap 1 metode OCTAVE Allegro dengan kolom nilai dampak. Kemudian tuliskan hasilnya pada kolom "Skor"
2. Nilai dampak (*value*) dikenal sebagai *high* = 3, *medium* = 2, dan *low* = 1
3. Menjumlahkan skor perkalian untuk mengetahui total skor risiko relatif

Tabel 7. *Area of Concern* Dokumentasi Laporan Proyek

<table>
<tr><td colspan="6">Information Asset Risk Worksheet</td></tr>
<tr><td rowspan="10">Information Asset Risk</td><td rowspan="8">Threat</td><td>Information Asset</td><td colspan="3">Dokumentasi laporan proyek</td></tr>
<tr><td>Area of Concern</td><td colspan="3">Pengungkapan atau penyebaran data informasi sensitif secara tidak sah
Server down
Serangan ransomware
Serangan Malware</td></tr>
<tr><td>Actor</td><td colspan="3">Engineer, Project manager, Quality Management Officer</td></tr>
<tr><td>Means</td><td colspan="3">Membagikan data confidential secara sengaja maupun tidak sengaja, data terkena ransomware dan tidak melakukan backup data secara rutin, data rusak terkena malware</td></tr>
<tr><td>Motive</td><td colspan="3">Kurangnya pemahaman terhadap pentingnya manajemen keamanan informasi,</td></tr>
<tr><td>Outcome</td><td colspan="3">✓ Disclosure ✓ Interruption
✓ Modification ✓ Destruction</td></tr>
<tr><td>Security Requirements</td><td colspan="3">Melakukan pembatasan hak akses, Melakukan backup data secara rutin, mendistribusikan aset melalui email perusahaan, meningkatkan fitur keamanan IT.</td></tr>
<tr><td>Probability</td><td>High</td><td>✓ Medium</td><td>Low</td></tr>
<tr><td colspan="2" rowspan="2">Consequences</td><td colspan="3">Severity</td></tr>
<tr><td>Impact Area</td><td>Value</td><td>Score</td></tr>
<tr><td colspan="2">Terganggunya produktivitas yang</td><td>Reputasi &</td><td>Medium</td><td>8</td></tr>
</table>

Jurnal Teknologi dan Informasi (JATI)
Volume 12 Nomor 2 Edisi September 2022
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v12i2

	mengakibatkan keterlambatan pengumpulan laporan proyek	kepercayaan *customer*		
		Financial	*Medium*	2
	Bila dokumen laporan proyek tersebut tersebar maka akan melanggar persetujuan kerahasiaan data	Produktifitas	*High*	9
		Keamanan & Kehidupan	*Low*	2
		Denda & sanksi hukum	*Medium*	10
Relative Risk Score				31

4.7 Tahap 8. Identify & Mitigate: Pilih Pendekatan Mitigasi

Tahap terakhir dari metode OCTAVE Allegro adalah melakukan pendekatan mitigasi dengan mengklasifikasikan setiap area perhatian yang teridentifikasi berdasarkan skor risiko relatif. Dimana matriks risiko relatif diperlukan. Tabel matriks risiko relatif digunakan untuk menentukan mitigasi risiko yang mengurutkan skor risiko relatif dari yang tertinggi hingga yang terendah. Tabel 8 menunjukkan tabel matriks risiko relatif.

Tabel 8. *Relative Risk Matrix*

Probability	*Risk Score*		
	30- 45	16-29	0-15
HIGH	POOL 1	POOL 2	POOL 2
MEDIUM	POOL 2	POOL 2	POOL 3
LOW	POOL 3	POOL 3	POOL 4

Untuk menentukan mitigasi risiko, pertama-tama sesuaikan rentang skor risiko pada tabel 8 sesuai dengan skor risiko relatif yang didapat dari tahapan lembar kerja *information asset risk* pada tabel 7. Dengan demikian, dapat disimpulkan bahwa pendekatan mitigasi sesuai dengan kategori POOL yang merupakan istilah untuk pengelompokan rentang skor risiko. Penentuan skor risiko ditentukan berdasarkan rentang skor risiko tertinggi yaitu 30-45 dikategorikan POOL 1, rentang skor risiko menengah dikategorikan POOL 2, dan rentang skor risiko terkecil dikategorikan POOL 3. Tabel 9 menunjukkan kisaran nilai untuk pendekatan mitigasi yang kemudian penentuan rekomendasi mitigasi ditunjukkan pada tabel 10.

Tabel 9. Penentuan Pendekatan Mitigasi

POOL	Pendekatan Mitigasi
POOL 1	*Mitigate*
POOL 2	*Mitigate or Defer*
POOL 3	*Defer or Accept*
POOL 4	*Accept*

Tabel 10. Mitigasi Risiko

Mitigasi Risiko			
Accept	*Defer*	*Mitigate*	*Transfer*
Rekomendasi Mitigasi			

Engineer	- Mengikuti training, edukasi terkait manajemen keamanan informasi - Melakukan prosedur backup terhadap dokumen laporan proyek - Memberlakukan checklist IT Compliance dalam melakukan pengelolaan data sebagai dokumentasi telah mengikuti kebijakan keamanan informasi - Implementasi Endpoint security pada device user
Project Manager	- Mengikuti training, edukasi terkait manajemen keamanan informasi - Melakukan prosedur backup terhadap dokumen laporan proyek - Memberlakukan checklist IT Compliance dalam melakukan pengelolaan data sebagai dokumentasi telah mengikuti kebijakan keamanan informasi - Implementasi Endpoint security pada device user
Quality Management Officer	- Mengikuti training, edukasi terkait manajemen keamanan informasi - Melakukan prosedur backup terhadap dokumen laporan proyek - Memberlakukan checklist IT Compliance dalam melakukan pengelolaan data sebagai dokumentasi telah mengikuti kebijakan keamanan informasi - Implementasi Endpoint security pada device user

4.8 Ringkasan Analisis Risiko PT. XYZ

Berdasarkan hasil analisis risiko OCTAVE Allegro dari 8 tahapan yang telah dilakukan, bahwa tindakan mitigasi untuk setiap aset informasi sesuai pada tabel 11.

Tabel 11. Mitigasi Risiko Aset Informasi PT.XYZ

Information Assets	Risk Mitigation Actions
Laporan Proyek	*Mitigate*

5. Kesimpulan

Berdasarkan hasil penelitian risiko keamanan informasi dengan menggunakan metode OCTAVE Allegro, penelitian ini telah berhasil mengidentifikasi risiko keamanan informasi pada perusahaan PT. XYZ terkait dengan sistem informasi manajemen. Sesuai dengan rumusan masalah penelitian, dapat disimpulkan hasil wawancara dan observasi termasuk studi literatur, mengidentifikasi 6 area perhatian yang berpotensi menimbulkan risiko keamanan informasi, yaitu pengungkapan atau penyebaran informasi sensitif yang tidak sah, fasilitas server down, serangan ransomware, serangan malware, kerusakan perangkat seperti laptop, dan kurangnya kesadaran dan pemahaman akan pentingnya keamanan informasi. Tingkat risiko yang diidentifikasi berdasarkan skor risiko relatif yang diperoleh dari perhitungan area of concern, prioritas dampak dan nilai dampak, terhadap dokumentasi laporan proyek pada tabel 7 menghasilkan skor risiko relatif 31 dan cukup tinggi berdasarkan rentang skor pada matriks risiko relatif yang mengacu pada ketentuan nilai rentang POOL yang diperoleh yaitu POOL 1. Dengan demikian risiko keamanan informasi terhadap dokumentasi laporan proyek mendapat kategori POOL 1 = high sehingga dibutuhkan pendekatan strategi mitigasi.

Daftar Pustaka

[1] R. Agusdinata and R. Noviana, “Risk Management Analysis of Public Services Information System Case Study: PT ABC,” *International Research Journal of Advanced Engineering and Science*, vol. 4, no. 3, pp. 442–444, 2019, [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-

[2] S. Rizky Wicaksono, C. Lenny Dwi Rizka, and G. Aprillia Immanuel, "Risk Assessment Menggunakan Pendekatan Octave Allegro (Studi Kasus: Schoology.com)," *Jurnal ICT: Information Communication & Technology*, vol. 18, no. 2, pp. 123–129, 2019, doi: 10.36054/jict-ikmi.v18i2.42.
[3] Gaol Ford and Supangkat Tito, "Risk management of electronic money (e-Money) using octave allegro methodology: Case study Pt. XYZ," *https://www.researchgate.net/journal/Far-East-Journal-of-Electronics-and-Communications-0973-7006*, 2017, doi: http://dx.doi.org/10.17654/EC017020259.
[4] C. Verbano and K. Venturini, "Managing Risks in SMEs: A Literature Review and Research Agenda," 2013. [Online]. Available: http://www.jotmi.org
[5] J. Freund and J. Jones, "Measuring and Managing Information Risk: A FAIR Approach," 2015.
[6] S. Amraoui, M. Elmaallam, H. Bensaid, and A. Kriouile, "Information Systems Risk Management: Litterature Review," *Computer and Information Science*, vol. 12, no. 3, p. 1, Jun. 2019, doi: 10.5539/cis.v12n3p1.
[7] Rivai Akbar, Suroso Jarot, and Pangemanan Firman, *ICIMTech 2020: proceedings of 2020 International Conference on Information Management and Technology (ICIMTech : 13-14 August 2020, Indonesia*. 2020.
[8] sen Jaydip, "Security and Security and Security and Security and Privacy Privacy Privacy Issues Issues Issues Issues in C in C in C in Cloud loud loud loud Computing Computing Computing Computing," 2013.
[9] P. Balozian and D. Leidner, "Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory," 2017.
[10] ECHO, "The COVID-19 Hackers Mind-set," *European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations*, pp. 1–8, 2020, [Online]. Available: https://echonetwork.eu/wp-content/uploads/2020/04/20200408-ECHO-WhitePaper-Hackers-Mindset-FINAL.pdf
[11] LP Singh, "Ergonomics for Working from Home during COVID-19 Pandemic," *Ergonomics International Journal*, vol. 4, no. 4, pp. 1–4, 2020, doi: 10.23880/eoij-16000246.
[12] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Computers and Security*, vol. 44, pp. 1–15, 2014, doi: 10.1016/j.cose.2014.04.005.
[13] L. Pan and A. Tomlinson, "A systematic review of information security risk assessment," *International Journal of Safety and Security Engineering*, vol. 6, no. 2, pp. 270–281, 2016, doi: 10.2495/SAFE-V6-N2-270-281.
[14] C. Evan, *OCTAVE and OCTAVE Allegro*. Software Engineering Institute, 2014.
[15] Suroso Jarot S. and Fakhrozi Muhammad A., "Assessment of Information System Risk Management with Octave Allegro at Education Institution," *Procedia Computer Science*, vol. 135, pp. 202–213, 2018, doi: 10.1016/j.procs.2018.08.167.