Analisis Risiko Keamanan Informasi Pada Divisi Penjualan Pt Matahari Department Store Cabang Jogja City Mall Menggunakan Metode Octave Allegro

1st Reza Fauzar Wahyu Pradana
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
rezafwp@student.telkomuniversity.ac.id

2nd Rio Guntur Utomo
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
riogunturutomo@telkomuniversity.ac.id

3rd Muhammad Al Makky
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
malmakky@telkomuniversity.ac.id

***Abstrak* — Keamanan informasi tidak bisa hanya difokuskan pada tools atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari setiap organisasi tentang apa yang harus dilindungi serta menentukan secara tepat mengenai solusi yang dapat menangani permasalahan kebutuhan keamanan informasi.Oleh sebab itu untuk mengantisipasi dampak risiko yang terjadi pada aset informasi di perusahaan, kerangka kerja yang akan digunakan adalah OCTAVE Allegro. Tujuan dari penelitian ini adalah melakukan tahapan proses analisis risiko keamanan informasi sesuai dengan kerangka kerja OCTAVE Allegro, mengetahui proses mitigasi risiko serta memberikan hasil rekomendasi kontrol terhadap penilaian risiko menggunakan pedoman ISO 27002:2013. Berdasarkan hasil penelitian dapat diketahui bahwa jumlah risiko yang berhasil diidentifikasi sebanyak 23 area dengan nilai tertinggi adalah 43. Hasil analisis menunjukkan bahwa 15 risiko akan dimitigasi (mitigate), 4 risiko akan ditangguhkan (defer), dan 4 risiko akan diterima (accept). Kemudian rekomendasi kontrol yang diberikan berdasarkan aspek people, process, dan technology.**

***Kata kunci*— Risiko, Keamanan Informasi, Aset Informasi, OCTAVE Allegro, ISO 27002:2013**

I. PENDAHULUAN

A. Latar Belakang

`Aset informasi merupakan aset yang dinilai penting bagi suatu organisasi yang perlu dilindungi dari risiko, baik dari luar maupun dalam. Keamanan informasi tidak bisa hanya difokuskan pada tools atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari setiap organisasi tentang apa yang harus dilindungi serta menentukan solusi secara tepat agar dapat menangani permasalahan kebutuhan keamanan informasi.Penggunaan teknologi informasi akan memunculkan risiko-risiko, maka pengelolaan terhadap risiko-risiko yang muncul merupakan hal yang perlu diperhatikan. Salah satu langkah awal dalam mengelola risiko adalah dengan melakukan penilaian risiko terhadap teknologi informasi.

Pada saat ini, divisi penjualan PT Matahari Department Store telah menerapkan suatu sistem informasi untuk mempermudah dalam menjalankan proses bisnis mereka yaitu Alphapos. Disamping itu, dalam menjalankan proses bisnisnya, perusahaan juga menggunakan pedoman ASEAN Corporate Governance Scorecard (ACGS) yang fokus terhadap bidang bisnis secara umum. Namun, pedoman ini tidak memiliki fokus terhadap risiko keamanan informasi. Oleh sebab itu, hingga saat ini penilaian risiko terhadap sistem informasi yang ada belum dilakukan.

Akibatnya muncul suatu masalah yaitu, sering terjadinya kebocoran password kepada pihak yang tidak berwenang. Terjadinya kebocoran password pada sistem informasi yang digunakan mengakibatkan tingkat keamanan pada sistem penjualan Alphapos terancam. Potensi ancaman yang ada seperti, adanya kebocoran informasi data penjualan perusahaan akibat penyalahgunaan password akses ke sistem penjualan Alphapos.

Oleh sebab itu untuk mengantisipasi dampak risiko yang terjadi pada aset informasi di perusahaan, salah satu kerangka kerja yang akan digunakan adalah OCTAVE Allegro. Metode OCTAVE Allegro berfokus pada aset informasi yang ada dalam organisasi atau perusahaan dalam lingkup bagaimana aset tersebut digunakan, di mana aset tersebut disimpan, dibawa, dan diproses serta bagaimana aset tersebut jika terkena ancaman, kerentanan, dan gangguan.

Penelitian ini akan difokuskan untuk mengidentifikasi penilaian analisis risiko keamanan informasi pada aset informasi serta mitigasi risiko keamanan informasi yang tepat untuk divisi penjualan di PT Matahari Department Store. Lalu di samping itu, penelitian ini juga memberikan rekomendasi kontrol kepada pihak perusahaan untuk menanggulangi serta mengurangi terjadinya risiko terhadap aset informasi.

1. Rumusan Masalah

Berdasarkan uraian latar belakang terdapat beberapa masalah yang menjadi acuan dalam penelitian ini, diantaranya adalah:

Bagaimana identifikasi penilaian risiko keamanan informasi pada divisi penjualan PT Matahari Department Store menggunakan OCTAVE Allegro?

Bagaimana mitigasi risiko keamanan informasi pada divisi penjualan PT Matahari Department Store menggunakan OCTAVE Allegro?

Bagaimana proses rekomendasi kontrol terhadap penilaian risiko keamanan informasi pada divisi penjualan PT Matahari Department Store?

II. KAJIAN TEORI

A. Landasan Teori

1. Risiko

Risiko merupakan akibat yang tidak/kurang menyenangkan (membahayakan dan merugikan) dari suatu tindakan atau perbuatan. Sehingga, risiko merupakan kemungkinan situasi yang dapat mengancam pencapaian tujuan serta sasaran dari sebuah organisasi.

2. Manajemen Risiko

Manajemen risiko merupakan serangkaian aktivitas yang dilakukan untuk mengelola mengontrol, dan mengurangi terjadinya suatu risiko pada organisasi/perusahaan, agar tidak mengalami kerugian.

3. Keamanan Informasi

Keamanan informasi adalah upaya yang dilakukan untuk melindungi aset informasi dari berbagai potensi ancaman. Keamanan informasi memiliki 3 aspek penting seperti:

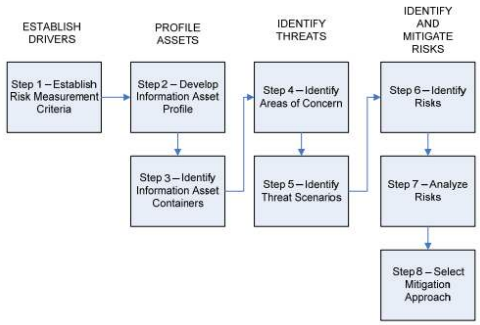
a. Confidentiality,
merupakan aspek yang menjamin bahwa suatu informasi tidak dapat di akses oleh pihak-pihak yang tidak berkepentingan.

b. Integrity,
merupakan aspek yang menjamin akurasi dan kelengkapan data informasi.

c. Availability,
merupakan aspek yang menjamin ketersediaan informasi yang dapat diakses oleh pihak yang berkepentingan.

4. OCTAVE Allegro

Metode OCTAVE Allegro berfokus pada aset informasi yang ada dalam organisasi atau perusahaan dalam lingkup bagaimana aset tersebut digunakan, di mana aset tersebut disimpan, dibawa, dan diproses serta bagaimana aset tersebut terkena ancaman, kerentanan, dan gangguan. Dalam metode OCTAVE Allegro terdapat empat fase yang dibagi menjadi 8 langkah yang dapat dilihat pada gambar di bawah ini.



GAMBAR 1
OCTAVE Allegro Roadmap

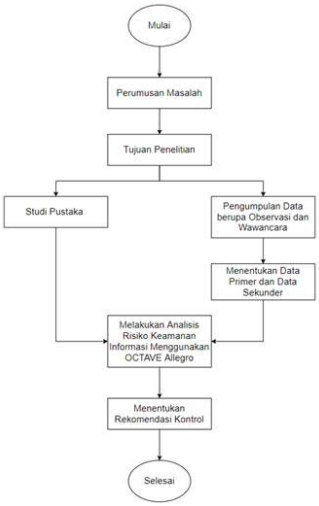
5. Standar ISO/IEC 27002:2013

Standar internasional ini dirancang untuk digunakan oleh organisasi sebagai referensi untuk memilih kontrol dalam proses penerapan Sistem Manajemen Keamanan Informasi (SMKI). SMKI melindungi kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi dengan menerapkan proses manajemen risiko dan memberikan kepercayaan kepada pihak yang berkepentingan bahwa risiko dikelola secara memadai.

III. METODE

A. Metode penelitian

Pada tahap ini menjelaskan bagaimana metode yang digunakan dalam penelitian ini dapat diimplementasikan terhadap data-data yang didapatkan.



GAMBAR 2
Flowchart Metodologi Penelitian

IV. HASIL DAN PEMBAHASAN

A. Analisis Data

Data yang telah dikumpulkan selanjutnya akan digunakan untuk proses analisis. Analisis tersebut akan dilakukan menggunakan metode OCTAVE Allegro.

1. Membangun Kriteria Pengukuran Risiko

Langkah pertama ini digunakan untuk mengevaluasi dampak risiko terhadap visi dan misi dari tujuan bisnis perusahaan. Kriteria pengukuran risiko ditentukan melalui area pada organisasi yang memiliki potensi terkena risiko.

TABEL 1
Kriteria pengukuran risiko - Reputasi dan Kepercayaan Pelanggan

Allegro Worksheet 1	Kriteria pengukuran risiko - Reputasi dan Kepercayaan Pelanggan		
Impact Area	**Low**	**Moderate**	**High**

Reputasi	Pengaruh terhadap reputasi perusahaan hampir tidak ada dan hanya dibutuhkan upaya-upaya kecil untuk	Reputasi perusahaan terdampak buruk dan perlu ekstra usaha dan biaya untuk melakukan perbaikan.	Pengaruh terhadap reputasi perusahaan sangat buruk dan dampaknya sangat kompleks sehingga
Kepercayaan Pelanggan (Customer Loyal)	Hilangnya kepercayaan pelanggan hampir tidak ada (<1%), karena permasalahan bisa diselesaikan ditempat dan pada saat itu	Hilangnya kepercayaan pelanggan >1% s/d <5% yang disebabkan penyelesaian masalah yang membutuhkan waktu lama.	Hilangnya kepercayaan pelanggan >5 % yang disebabkan penyelesaian masalah yang tidak tuntas.

2. Mengembangkan Profil Aset Informasi

Pada tahap ini diawali dengan melakukan dokumentasi pada lembar kerja 8 terhadap aset yang dinilai kritikal sesuai dengan kriteria pada OCTAVE Allegro. Proses ini menjelaskan setiap informasi pada aset yang ada dan mendefinisikan persyaratan keamanan untuk aset tersebut.

TABEL 2
Profil Aset Informasi

Allegro Worksheet 8a	**Critical Information Asset Profile**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
1. Data Penjualan	2. Data ini sangat penting untuk mengetahui pencapaian target	Data terkait penjualan produk meliputi penjualan gross, penjualan net, diskon
(4) Owner(s) *Who owns this information asset?*		
Finance & IT Dept di masing masing unit bisnis di perusahaan		
(5) Security Requirements *What are the security requirements for this information asset?*		
● **Confidentiality**	Only authorized personnel can view this information	Data ini merupakan rahasia perusahaan yang tidak boleh diketahui oleh
● **Integrity**	Only authorized personnel can modify this information	Data ini real terkait informasi performa dari penjualan produk yang tidak boleh
● **Availability**	This asset must be available for these personnel to do their jobs, as follows: 3. This asset must be available for	Data ini terbentuk otomatis pada system alphapos ketika terjadi transaksi di mesin POS Register. Data ini tersaji dalam periode hourly(jam), daily(per tanggal), weekly (periode
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
4. Confidentiality	5. (v) Integrity	6. Availability

3. Mengidentifikasi Asset Container

Pada tahap ini akan dilakukan proses identifikasi pada semua *container* (wadah) aset informasi yang ada. *Asset container* adalah tempat dimana aset informasi tersebut disimpan, diproses dan dikirim.

TABEL 3
Kontainer Aset(*Technical*)

Allegro Worksheet 9a	**INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)**
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Database : Data Penjualan Data disimpan di Server Primer dan Server Backup yang ada di toko (Unit Bisnis)	Finance & IT Dept Toko
2. Aplikasi : ALPHAPOS Data penjualan diakses menggunakan aplikasi ALPHAPOS yang ada di toko (Unit Bisnis)	Finance & IT Dept di Toko
3. Perangkat Keras : Komputer/ Server Perangkat keras yang digunakan untuk mengakses portal ALPHAPOS adalah perangkat Komputer dengan jaringan internet dan LAN	Finance & IT Dept di Toko
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Database : Data Penjualan Data disimpan di Server Primer dan Server Backup yang ada di Kantor Pusat (Head Office)	Finance & IT Dept di Kantor Pusat (Head Office)
2. Aplikasi : ALPHAPOS Data penjualan diakses menggunakan aplikasi ALPHAPOS yang ada di Kantor Pusat (Head Office)	Finance & IT Dept di Kantor Pusat (Head Office)
3. Perangkat Keras : Komputer/Server Perangkat keras yang digunakan untuk mengakses portal ALPHAPOS adalah perangkat Komputer dengan jaringan internet dan LAN	Finance & IT Dept di Kantor Pusat (Head Office)

TABEL 4
Kontainer Aset(*Physical*)

Allegro Worksheet 9b - Data Penjualan	**Information Asset Risk Environment Map (Physical)**
Internal	
Container Description	**Owner(s)**
1. Barcode Produk Barcode pada label produk diinput/dilakukan scanner oleh petuigas kasir di mesin POS Register untuk memproses transaksi penjualan.	Finance & IT Dept di Toko
2. POS Register Online Data penjualan terproses otomatis ketika terjadi transaksi penjualan melalui Mesin POS Register yang terkoneksi dengan Server Alphapos di Toko	Finance & IT Dept di Toko

3. End of Day Prosessing Data penjualan terproses otomatis dan tersimpan di Server HO ketika toko melakukan End of Day Prosessing melalui Komputer/Server yang ada di Toko	Finance & IT Dept di Toko
External	
Container Description	**Owner(s)**
1. Konfirmasi End of Day Prosessing Komputer Server di Head Office memberikan konfirmasi End of Day Prosessing data penjualan sukses.	Finance & IT Dept di Head Office

TABEL 5
Kontainer Aset(*People*)

Allegro Worksheet 9c - Data Penjualan	**Information Asset Risk Environment Map (People)**
Internal	
Name or Role/Responsibility	**Department or Unit**
1. Kasir (Role Staff)	Finance & IT Dept di Toko
2. Supervisor (Role Manager)	Finance & IT Dept di Toko
3. Assisten Store Manager (Role Auxilary)	Finance & IT Dept di Toko
4. Store Manager (Role Auxilary)	Finance & IT Dept di Toko
External	
Contractor, Vendor, Etc.	**Organization**
1. Admin FA	Finance & Accounting Head Office
2. Admin IT Dept	IT Dept Head Office

4. Mengidentifikasi Area of Concern

Pada tahap ini akan dilakukan proses identifikasi terhadap hal-hal yang berpengaruh terhadap aset informasi kritis.

TABEL 6
Area Of Concern

No	Area Of Concern - Data Penjualan
1	Penyalahgunaan user akses oleh pihak lain yang tidak mempunyai kewenangan mengakses informasi
2	Data penjualan tidak bisa diakses karena gangguan jaringan
3	Informasi data penjualan tidak akurat karena gagal sending transaksi (proses End of Day gagal)
4	Kehilangan data penjualan karena serangan virus dan server backup tidak berfungsi
5	Informasi data penjualan tidak dapat di akses karena terjadi masalah pada sistem aplikasi Alphapos
6	Penyebaran informasi data penjualan secara manual melalui proses cetak kepada pihak luar organisasi

5. Mengidentifikasi Skenario Ancaman

Pada tahap ini *area of concern* akan diperluas menjadi skenario ancaman yang lebih rinci terhadap *threat properties.*

TABEL 7
Identifikasi Skenario Ancaman

1	Information Asset	Data Penjualan
	Area of Concern	Penyalahgunaan user akses oleh pihak lain yang tidak mempunyai kewenangan mengakses informasi
	(1) Actor	Staf Admin
	(2) Means	Staf Admin melihat dan menghafal user dan password otorisasi pada saat pemilik user membuka data.
	(3) Motive	Dengan sengaja ingin mengambil data
	(4) Outcome	[v] Disclosure [v] Modification [ ] Destruction [v] Interruption
	(5) Security Requirement	User wajib melakukan penggantian password akses secara berkala dan tidak boleh memberitahukan password akses kepada orang lain
	(6) Probability	Medium

6. Mengidentifikasi Risiko

Pada tahap ini akan dilakukan proses identifikasi risiko dengan menjelaskan segala bentuk konsekuensi yang akan terjadi apabila skenario ancaman yang telah di identifikasi sebelumnya terjadi.

TABEL 8
Identifikasi Risiko

Data Penjualan		
1	**Area of Concern**	Penyalahgunaan user akses oleh pihak lain yang tidak mempunyai kewenangan mengakses informasi
	Consequences	
	Perusahaan mengalami kerugian apabila pelaku penyalahgunaan membuat kerusakan data karena data menjadi tidak akurat dan menyebabkan selisih penjualan yang mengakibatkan komplain dari pihak suplier	

7. Analisis Risiko

Pada tahap ini akan dilakukan proses penilaian skor risiko relatif untuk setiap risiko pada aset informasi yang ada. Skor risiko relatif diperoleh dengan mempertimbangkan sejauh mana konsekuensi risiko berpengaruh terhadap organisasi. Penilaian ini akan digunakan untuk menentukan risiko pada aset mana yang akan dimitigasi.

TABEL 9
Nilai Impact Area

Impact Area	Priority	Low (1)	Medium (2)	High (3)
Reputasi dan Kepercayaan Pelanggan	**4**	4	8	12
Keuangan	**5**	5	10	15
Produktivitas	**2**	2	4	6
Keamanan dan Kesehatan	**1**	1	2	3
Denda dan Penalti	**3**	3	6	9
Akurasi Data	**4**	4	8	12
Total	**19**	**19**	**38**	**57**

Pada lembar kerja 10 OCTAVE Allegro akan dilakukan dokumentasi dari seluruh kegiatan yang telah dilakukan mulai dari tahap empat hingga tahap ketujuh.

TABEL 10
Allegro Worksheet 10

Allegro -		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk		Information Asset	Data Penjualan		
		Area of	Penyalahgunaan user akses oleh pihak lain yang		
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Staf Admin		
		(2) Means *How would the actor do it? What would they do?*	Staf Admin melihat dan menghafal user dan password otorisasi pada saat pemilik user membuka data.		
		(3) Motive *What is the actor's reason for doing it?*	Dengan sengaja ingin mengambil data		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ✓ **Modification** ✓ **Destruction** ✓ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	User wajib melakukan penggantian password akses secara berkala dan tidak boleh memberitahukan password kepada orang lain.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	**High**	✓ **Medium**	**Low**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Value**	**Score**
	Perusahaan mengalami kerugian apabila pelaku penyalahgunaan membuat kerusakan data karena data menjadi tidak akurat dan menyebabkan selisih penjualan		Reputation	High	12
			Financial	High	15
			Productivity	Medium	4
			Safety &	Low	1
			Fines &	Low	3
			yang mengakibatkan komplain dari pihak suplier	Akurasi Data	Medium	8
					Relative Risk Score	**43**

8. Memilih Pendekatan Mitigasi

Tahap ini dilakukan dengan memprioritaskan risiko, memutuskan pendekatan untuk memitigasi risiko penting berdasarkan sejumlah faktor organisasi, dan mengembangkan strategi mitigasi dengan mempertimbangkan nilai aset tersebut.

TABEL 11
Relative Risk Matrix

Relative Risk Matrix			
Probability	**Risk Score**		
	30 to 45	**16 to 29**	**0 to 15**
High	POOL 1	POOL 2	POOL 2
Medium	POOL 2	POOL 2	POOL 3
Low	POOL 3	POOL 3	POOL 4

TABEL 12
Pendekatan Mitigasi

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

TABEL 13
Hasil Mitigasi Risiko

Area of Concern	Mitigation Approach
Data Penjualan	
Penyalahgunaan user akses oleh pihak lain yang tidak mempunyai kewenangan mengakses informasi	Mitigate
Data penjualan tidak bisa diakses karena gangguan jaringan	Accept
Informasi data penjualan tidak akurat karena gagal sending transaksi (proses End of Day gagal)	Mitigate
Kehilangan data penjualan karena serangan virus dan server backup tidak berfungsi	Mitigate
Informasi data penjualan tidak dapat di akses karena terjadi masalah pada sistem aplikasi Alphapos	Defer
Penyebaran informasi data penjualan secara manual melalui proses cetak kepada pihak luar organisasi	Mitigate

9. Rekomendasi Kontrol

Pada bagian ini menjelaskan mengenai pemberian rekomendasi kebijakan kontrol menggunakan ISO 27002:2013 berdasarkan risiko yang telah diidentifikasikan sebelumnya.

TABEL 14
Rekomendasi Kontrol Risiko

Area of Concern	ISO 27002:2013	Kontrol
Data Penjualan		
Penyalahgunaan user akses oleh pihak lain yang tidak mempunyai kewenangan mengakses informasi	● A.7.2.2 Information security awarness, education and training ● A.7.2.3 Disciplinary process ● A.9.1.1 Access control policy ● A.9.3.1 Use of secret authentication information ● A.9.4.1 Information access restriction ● A.12.6.1 Management of technical vulnerabilities	● Semua karyawan organisasi harus menerima pendidikan dan pelatihan kesadaran yang sesuai dan pembaruan rutin dalam kebijakan dan prosedur organisasi, yang relevan dengan fungsi pekerjaan mereka. (A.7.2.2) ● Harus ada proses pendisiplinan yang formal dan dikomunikasikan untuk mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran keamanan informasi (A.7.2.3) ● Kebijakan kontrol akses harus ditetapkan, didokumentasikan, dan ditinjau berdasarkan persyaratan bisnis dan keamanan informasi. (A.9.1.1) ● Akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses. (A.9.4.1)

10. Rekomendasi Aspek

Pada tahap ini akan diberikan rekomendasi aspek terhadap tiga aspek, yaitu *people, process* dan *technology.*

TABEL 15
Rekomendasi Aspek

ISO 27002:2013	Aspek		
	People	**Process**	**Technology**
A.7.2.2 Information security awarness, education and training	Memberikan pelatihan kepada karyawan organisasi mengenai pentingnya kesadaran keamanan informasi		
A.7.2.3 Disciplinary process	Memberikan tindakan tegas terhadap karyawan yang melakukan pelanggaran keamanan informasi	Menetapkan kebijakan mengenai pelanggaran keamanan informasi	
A.9.4.1 Information access restriction		Menetapkan kebijakan tentang siapa saja yang berwenang mengakses informasi	Membatasi akses ke aset informasi hanya untuk yang memiliki wewenang saja

V. KESIMPULAN

A. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan menggunakan metode OCTAVE Allegro, dapat disimpulkan bahwa:

Dari penggunaan metode *OCTAVE Allegro*, telah diidentifikasi 6 area dampak serta 4 aset informasi kritis yang berhasil diidentifikasi. Jumlah risiko yang berhasil diidentifikasi sebanyak 23 area dengan nilai risiko tertinggi adalah 43.

Hasil analisis menunjukkan bahwa 15 risiko akan dimitigasi (*mitigate*), 4 risiko akan ditangguhkan (*defer*), dan 4 risiko akan diterima (*accept*).

Rekomendasi kontrol diberikan berdasarkan 3 aspek, yaitu *people*, *process*, dan *technology.*

B. Saran

Adapun saran yang dapat diberikan pada penelitian selanjutnya adalah melakukan perbandingan pada hasil analisis saat ini dengan menggunakan metode analisis risiko yang lainnya seperti NIST SP 800-30 untuk mengetahui hasil analisis risiko dari setiap metode yang digunakan.

REFERENSI

1. Caralli. Richard A., Stevens, James F., Young, Lisa R., & Wilson, William R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, May 2007.
2. Driantami, Hana Talitha Iddo., Suprapto, & Perdanakusuma, Andi Reza. (2018). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi Kasus Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square).
3. Suprandono, Bambang. (2009). Manajemen Keamanan Informasi Dengan Menggunakan Metode OCTAVE. Teknik Elektro Universitas Muhammadiyah Semarang..
4. Saputra, Rizky Ramadhan., Setiawan, Eman., & Ambarwati, Awalludiyah. (2019). Manajemen Risiko Teknologi Informasi Menggunakan Metode OCTAVE Allegro pada PT. Hakiki Donarta Surabaya. pp. 1-10.
5. Sitorus, Greenhard., Fauzi. Rokhman., & Nugraha, Ryan Adhitya. (2020). Analisis Risiko Keamanan Informasi Menggunakan Metode OCTAVE Allegro Pada Dinas Komunikasi Dan Informatika Jawa Barat.
6. A. Ramadhintia, Raihan., Bisma, Rahadian. (2021). Analisis Manajemen Risiko Aplikasi Ujian Online Dengan Metode OCTAVE Allegro Pada Lembaga Pendidikan.

7. Novrian, Nurzami., Fauzi, Rokhman., & Ramdani, Lutfhi. (2021) Analisis Keamanan Informasi Dalam Bisnis Proses Fulfillment Layanan Indihome Menggunakan Metode OCTAVE Allegro Pada Divisi IT PT. Telkom Indonesia Tbk.
8. ISO/IEC. 2013. ISO/IEC 27002 Information Technology – Security Techniques – Code Of Practice For Information Security Controls: ISO/IEC
9. ISO. (2009). AS/NZS ISO 31000:2009 Risk Management, Principles and Guidelines. ISO 2009.
10. Firmansyah, H. (2014). Implementasi framework manajemen risiko terhadap penggunaan teknologi informasi perbankan. *Seminar Dan Call Paper Munas Aptikom*, *10*, 172–178.
11. Puriwigati, A. N., & Buana, U. M. (2020). *Sistem Informasi Manajemen-Keamanan Informasi*. *May*.
12. Anshori, F. A., & 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.
13. Matahari. " Tentang Matahari ". https://www.matahari.com/corporate/about-us. (diakses 24 April 2022 09.00).