Jurnal Ilmu Komputer Indonesia (JIK) , Volume 7 , No : 1, Februari 2022
p-ISSN : 2615-2703 (Print) dan e-ISSN: 2615-2711 (Online)

ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO DAN ANALYTICAL HIRARCHY PROCESS PADA DATA CENTER PEMERINTAH KABUPATEN BULELENG

Nyoman Budarsa[1],G Indrawan[2], Aris Gunadi [3]

Program Studi Ilmu Komputer Pasca Sarjana Undiksha
Jl. Udayana No. 11Singaraja, Bali, Indonesia

[1]gbudarsa@gmail.com

Abstrak

Penggunaan teknologi informasi dan komunikasi dalam bidang pemerintahan merupakan suatu hal yang penting untuk mendukung sistem pemerintahan berbasis elektronik. Data center merupakan pusat dari infrastruktur teknologi informasi yang memiliki peran yang sangat strategis yang menentukan kelangsungan sistem pemerintahan berbasis elektronik untuk pelayanan publik dan administrasi pemerintahan. Namun, dalam impelementasi sistem pemerintahan berbasis elektronik pada data center Pemerintah Kabupaten Buleleng terdapat peluang munculnya risiko keamanan informasi yang mengakibatkan terganggunya pelayanan publik dan administrasi pemerintahan. Aspek keamanan informasi ini meliputi aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Penelitian ini bertujuan untuk menghasilkan analisis risiko keamanan teknologi informasi dan komunikasi pada instansi pelayanan publik. Metode yang digunakan untuk analisis risiko keamanan informasi ini adalah OCTAVE Allegro karena metode ini sangat sesuai dengan karakteristik pada instansi pemerintah. Sebagai tindak lanjut dari hasil profil risiko yang dihasilkan, selanjutnya diolah sistem penunjang keputusan, yaitu Analitic Hirarchy Process (AHP). Hasil penelitian ini diharapkan dapat dijadikan pedoman dalam kebijakan pengelolaan data center pada instansi pemerintah.

***Kata- kata kunci* : keamanan informasi, OCTAVE Allegro, AHP**

Abstract

The use of information and communication technology in the field of government is an important thing to support an electronic-based government system. The data center is the center of information technology infrastructure which has a very strategic role in determining the continuity of an electronic-based government system for public services and government administration. However, in the implementation of an electronic-based government system in the Buleleng Regency Government's data center there is an opportunity for information security risks to arise which result in disruption of public services and government administration. This aspect of information security includes aspects of confidentiality, integrity, and availability. This study aims to produce an analysis of information and communication technology security risks in public service agencies. The method used for information security risk analysis is OCTAVE Allegro because this method is very suitable for the characteristics of government agencies. As a follow-up to the resulting risk profile results, it is then processed by a decision

upport system, namely the Analytical Hierarchy Process (AHP). The results of this study are expected to be used as guidelines in data center management policies in government agencies.

Keywords : Information Security , OCTAVE Allegro, AHP

I. PENDAHULUAN

Penggunaan teknologi informasi dan komunikasi dalam bidang pemerintahan merupakan suatu hal yang penting untuk mendukung sistem pemerintahan berbasis elektronik. Data center merupakan pusat dari infrastruktur teknologi informasi yang memiliki peran yang sangat strategis yang menentukan kelangsungan sistem pemerintahan berbasis elektronik untuk pelayanan publik dan administrasi pemerintahan.

Pemerintah Kabupaten Buleleng memiliki data center yang berada di Dinas Komunikasi Informatika Persandian dan Statistik yang di dalamnya terdapat infrastruktur teknologi informasi seperti komputer server dan perangkat jaringan. Terdapat 12 (dua belas) server fisik yang digunakan untuk menampung sistem informasi untuk pelayanan publik dan administrasi pemerintahan.

Namun, dalam impelementasi sistem pemerintahan berbasis elektronik pada data center Pemerintah Kabupaten Buleleng terdapat peluang munculnya risiko keamanan informasi yang mengakibatkan terganggunya pelayanan publik dan administrasi pemerintahan. Aspek keamanan informasi ini meliputi aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Keamanan informasi tidak hanya tergantung pada alat dan teknologi, akan tetapi membutuhkan kesadaran dalam organisasi tentang apa yang harus dilindungi dan pemilihan solusi yang tepat untuk menangani masalah dalam kebutuhan keamanan informasi(Jufri et al., 2018).

Diperlukan analisis risiko keamanan informasi untuk mengetahui adanya ancaman dan kerentanan informasi sehingga dapat ditentukan peringkat risiko dari yang terbesar samapi yang terkecil. Hasil analisis risiko ini dapat dijadikan acuan dalam membuat perencanaan pengelolaan data center serta sebagai penunjang keputusan ketika terjadi gangguan dalam implementasi sistem pemerintahan berbasis elektronik. Beberapa permasalahan yang yang sering dialami oleh pengguna data center pemerintah Kabupaten Buleleng antara lain, server tidak dapat diakses dari beberapa pengguna, adanya peretasan terhadap aplikasi yang berbasis website, dan lambatnya koneksi ke aplikasi pelayanan publik maupun administrasi pemerintahan.

Ada banyak metode penilaian risiko yang tersedia, diantaranya Panduan untuk Melakukan Penilaian Risiko (Institut Nasional Standard dan teknologi [NIST],2012, COBIT, ISO 27005 dan OCTAVE. Penelitian ini menfokuskan pada analisis, identifikasi dan penilaian risiko keamanan informasi pada Data Center Pemerintah Kabupaten Buleleng menggunakan metode OCTAVE Allegro dan Analytical Hirarchy Process.(Prajanti & Ramli, 2019). Penggunaan dua metode ini diharapkan dapat memberikan hasil berupa peringkat risiko yang lebih cepat, akurat, dan bisa diterapkan sesuai dengan kondisi khususnya pada instansi pemerintah.

II. TINJAUAN PUSTAKA

Analisis Risiko

Pengukuran risiko keamanan informasi adalah pekerjaan yang sulit dilakukan secara akurat pada sebuah sistem informasi. Analisis risiko dapat menggunakan pendekatan kuantitif dan kualitatif. Pada pendekatan kuantitatif terdapat tahapan penilaian dari masing – masing asset. Untuk mendapatkan niali asset seperti informasi atau database, sangat

terbuka peluang munculnya subjektifitas penilai. Karena dalam proses penilaian tersebut terdiri dari elemen yang harus ditaksir.

Sementara metode pendekatan kualitatif menggunakan kuesioner untuk mendapatkan fakta melalui perkiraan secara statistic dengan hasil low, medium dan high sehinggan ada kesulitan untuk menghitung kerugian finansial jika hanya berdasar pada asumsi.

Analisis risiko menggunakan pendekatan kualitatif sangat diominasi oleh pengukuran subjektif, sedangkan pendekatan kuantitatif dapat menghilangkan sifat subjektif yang ada (Mazareanu, 2011). Metode kuantitatif lebih objektif dibandingkan motode kualitatif.

Manajemen risiko adalah bagian dari manajem sistem informasi yang ditujukan untuk menilai bagaimana ancaman dan kerentanan sistem informasi dan aset yang dimiliki. (Sardjono & Cholik, 2018). Manajemen risiko dapat mengurangi risiko seperti proses bisnis yang tidak optimal, pemborosan anggaran dan turunnya reputasi institusi.(Suroso & Fakhrozi, 2018).

Menurut Rhoes pada tahun 2013 mengurangi risiko tidak berarti menghilangkannya, tetapi menurunkan tingkat risiko ke tingkat yang dapat diterima oleh organisasi tersebut. Untuk menjamin keamanan informasi, mengelola dan mengantisipasi risiko secara efektif diperlukanan alisis risiko, definisi ancaman dan dampak atau akibat yang ditimbulkan oleh risiko tersebut.

Dengan melakukan analisis dan identifikasi terhadap risiko yang ada, hal ini dapat memberikan strategi yang tepat untuk keamanan informasi dan mengurangi peluang munculnya area risiko berdampak pada asset – asset penting atau rahasia yang tidak terlindungi. Fokus pada evaluasi asset yang dimiliki adalah kunci keberlangsungan perusahaan.(Dorofee, 2005b). Tujuan melakukan analisis terhadap risiko adalah untuk memberikan gambaran terhadap peluang munculnya ancaman yang bisa terjadi sehingga organisasi bisa menyusun strategi dan langkah untuk mitigasi dan evaluasi risiko. Hasil analisis risiko dapat digambarkan ke dalam matrik risiko.

Data Center

Data center adalah kumpulan server dan sistem penyimpanan data yang membutuhkan fasilitas khusus untuk menampung sumber daya yang dimiliki.(Riasetiawan, 2016) Pusat penampungan data ini memiliki criteria khusus dalam perancangannya, antara lain :

a. *Aviability*, yaitu mampu menjalankan opersi secara berkelanjutan dan terus menerus dalam kondisi apapun.
b. *Scalability*, yaitu mampu berdaptasi dengan penambahan kebutuhan dan teknologi baru tanpa merubah substansi data center secara keseluruhan.
c. *Security*, data center mampu melindungi asset data yang tersimpat pada server secara fisik maupun non fisik.

Keamanan Informasi

Informasi merupakan aset yang sangat penting bagi organasisasi terutama instansi pemerintah. Keamanan informasi adalah usaha untuk melindungi aset informasi dalam segala bentuknya, baik tertulis, lisan, elektronik, grafis, dan lain-lain. Keamanan informasi diusahakan untuk mencapai tiga sasaran utama yaitu aspek kerahasiaan, ketersediaan, dan ketersediaan informasiserta mencegah dan mengurangi hal-hal yang dapat terjadi seperti kerusakan, kehilangan atau juga informasi yang bersifat pribadi bisa tersebar ke pihak yang tidak berkepentingan.

Ada tiga komponen yang memberi kontribusi kepada risiko keamanan informasi, yaitu asset (aset), vulnerabilities (kelemahan), dan threats (ancaman)(Rahardjo, 1998). Aset terdiri dari infrastruktur perangkat keras, perangkat lunak, dokumentasi, data, lingkungan dan manusia. Kelemahan meliputi *software bugs*, radiasi, *tapping*,

hard copy, keteledoran dan media penyimpanan, Sementara ancaman meliputi pemakai, kecelakaan, dan *crackers*.

Keamanan informasi bagi instansi pelayanan publik sangat penting artinya karena akan mempengaruhi keberlangsungan pelayanan publik.

Metode OCTAVE Allegro

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) merupakan pendekatan untuk mengelola dan analisis risiko keamanan teknologi informasi. yang dikembangkan oleh Software Enginerring Insitute Universitas Carnegie Mellon. OCTAVE memiliki seperangkat peralatan, teknik, dan metode untuk penilaian dan perencanaan keamanan informasi. OCTAVE memiliki tiga varian, yaitu OCTAVE, OCTAVE S, dan OCTAVE Allegro. Ketiga metode tersebut bukanlah untuk saling melengkapi atau mengantikan satu dengan yang lain, namun untuk memenuhi kebutuhan sfesifik dari pengguna OCTAVE yang akan melakukan penilaian risiko.

Metode OCTAVE adalah versi OCTAVE yang pertama kali dikembangkan. Metode OCTAVE dilaksanakan dengn mengadakan serangkaian workshop dan difasilitasi oleh tim analisi yang dibuat pada organisasi atau departemen teknologi informasi. Metode ini ditujukan untuk perusahaan besar yang memiliki lebih dari 300 karyawan.

OCTAVE menggunakan pendekatani tiga tahap dengan menguji isu – isu organisasi dan teknologi terhadap penyusunan masalah yang komperhensif berdasarkan kebutuhan keamanan informasi suatu organisasi.

Gambar.1. Metode OCTAVE

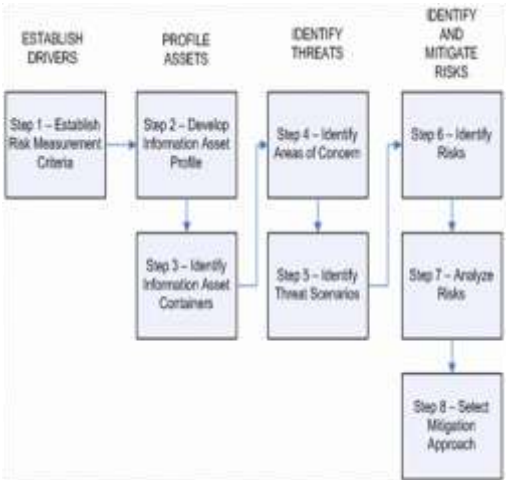
Dari gambar 1. diatas, metode OCTAVE dimulai pada tahap 1, yaitu tim analisis melakukan identifikasi aset informasi yang penting dan strategi perlindungan saat ini untuk asset dimaksud. Selanjutnya menentukan aset mana yang paling penting bagi organisasi, dokumen persyaratan keamanan informasi yang ada, dan melakukan identifikasi ancaman. Pada tahap 2, tim analisis melakukan evaluasi terhadap infrastruktur unttuk melengkapi analisis ancaman pada tahap 1. Pada tahap 3, tim analisis melakukan identifikasi dan membuat mitigasi risiko untuk aset yang bernilai kritis(Dorofee, 2005a).

Sama seperti metode OCTAVE, OCTAVE-S juga terdiri dari tiga tahapan. Namun, pada metode OCTAVE-S dilakukan oleh tim analisis yang memiliki pengetahuan yang mendalam tentang perusahaan atau organisasi. OCTAVE-S tidak menggunkan informasi yang didapatkan dari workshop karena OCTAVE-S menggunakan asumsi bahwa timanalisis sudah memiliki pengetahuan tentang aset penting yang berkaitan dengan informasi, kebutuhan keamanan, ancaman dan prosedur keamaanan informasi yang ada pada organisasi.

OCTAVE Allegro bertujuan untuk melakukan penilaian luas terhadap lingkungan risiko operasional dalam suatu organisasi tanpa perlu pengetahuan yang luas dalam hal penilaian risiko. Kata Allegro berarti dalam tempo yang lincah(Keating, 2014). Metode ini menggunakan pengetahuan seseorang

tentang praktik dan proses keamanan informasi pada sebuah organisasi untuk melihat keadaan praktik keamanan saat ini pada organisasi.

OCTAVE Allegro merupakan sebuah kerangka kerja yang menggunakan pendekatan OCTAVE dan didesain untuk melakukan penilaian risiko terhadap operasional organisasi atau perusahaan. Tujuannya adalah untuk menghasilkan hasil penilaian profil risiko yang lebih cepat tanpa memerlukan pengetahuan mendalam terkait penilaian risiko atau audit. (Caralli et al., 2007). OCTAVE Allegro sedikit memiliki perbedaan jika dibandingkan dengan pendekatan OCTAVE lainnya karena framework ini fokus pada aset informasi yang oleh instansi dalam konteks bagaimana aset tersebut digunakan, bagaimana asset informasi ini disimpan, dipindahkan, dan diproses. Disamping juga bagaimana ancaman, kerentanan, dan gangguan dapat terjadi pada aset tersebut. *Framework* OCTAVE Allegro terdiri atas delapan tahapan yang diklasifikasikan menjadi empat fase.



Gambar 2.. Tahapan OVTAVE Allegro

Metode OCTAVE Allegro adalah salah satu contoh evaluasi yang konsisten dengan prinsip, atribut dan output.(Dorofee, 2005a) Metode ini bisa mengasilkan profil risiko dengan atribut yang konsisten sehingga dapat digunakan untuk proses pengambilan keputusan selanjutnya.

Instansi pemerintah memiliki karakteristik yang khusus terkait pengelolaan anggaran, sumber daya manusia dan waktu pengelolaan risiko keamanan informasi. OCTAVE Allegro bisa diterapkan pada organisasi dengan sumber daya seperti pada instansi pemerintah.(St et al., 2020)

III. METODE PENELITIAN

Metode OOCTAVE Allegro

Metode analisis data yang digunakan dalam penelitian ini dengan mengisi semua worksheet sesuai dengan kerangka kerja OCTAVE Allegro. Ada empat tingkatan dengan delapan langkah dalam melakukan penilaian risiko keamanan terhadap asset informasi. Proses ini akan menghasilkan sepuluh tabel *worksheet* hasil penilaian. Dari hasil tahapan identifikasi risiko mengacu pada asset risk worksheet OCTAVE Allegro maka akan didapatkan tabel area terdampak.

Metode AHP

Selanjutnya adalah membuat matrix inisiasi berdasarkan nilai dari *worksheet* nomor 10 yang akan menjadi input dalam menghitung rating dari AHP.

Menggunakan metode AHP, maka dapat dibuat urutan dari seluruh area perhatian yang didapatkan pada tahapan identifikasi. Peringkat risiko diurutkan berdasarkan pada nilai yang terbesar.

IV. EXPERIMENT AND RESULT

Sebelum memulai penilaian risiko, peneliti melakukan mengumpulkan data dan informasi mengenai pengelolaan data center Pemerintah Kabupaten Buleleng yang ada pada Dinas Komunikasi Informatika Persandian dan Statistik di Bidang Infrastruktur dan Layanan Sistem

Pemerintahan Berbasis Elektronik. Proses wawancara dilakukan untuk mendapatkan informasi tentang aset operasional yang dianggap penting oleh organisasi.

OCTAVE Allegro Risk Assesment

Ada delapan Langkah yang harus dilakukan untuk melakukan analisi risiko sesuai dengan kertas kerja dari OCTAVE Allegro.

Langkah 1 - Menetapkan Kriteria Pengukuran Risiko

Terdapat dua aktivitas pada langkah ini, yang diawali dengan mengevaluasi dampak risiko dengan mengukur semua aspek kriteria penetapan risiko menggunakan tabel kertas kerja dari OCTAVE Allegro.

Penetapan kriteria penilaian risiko ditetapkan berdasarkan area terdampak meliputi :

a. Reputasi dan kepercayaan pengguna
b. Keuangan
c. Produktifitas organisasi
d. Keselamatan dan kesehatan pegawai
e. Denda dan tuntutan hukum

Langkah 2 – Membuat Profil Aset Informasi.

Terdapat delapan kegiatan yaitu yang pertama adalah melakukan identifikasi aset informasi dan dilanjutkan dengan melakukan penilaian risiko tersetruktur pada aset yang dinilai kritis. Kegiatan ketiga dan keempat adalah pengumpulan informasi yang dinilai penting selanjutnya membuat dokumentasi alasan pemilihan aset kritis. Kegiatan kelima dan keenam adalah membuat deskripsi aset informasi kritis selanjutnya melakukan identifikasi kepemilikan aset informasi kritis tersebut. Kegiatan ketujuh dan kedelapan adalah mengisi kebutuhan keamanan untuk aspek keamanan informasi yaitu kerahasiaan, integritas, dan ketersediaan.

Semua hasil dari langkah kedua ini didokumentasi pada tabel profil aset kritis

Langkah 3 – Mengidentifikasi Kontainer Aset Informasi

Kegiatan pada langkah ketiga ini adalah melakukan identifikasi kontainer atau wadah dimana aset informasi disimpan, dikirim dan diproses.

Langkah 4 – Mengidentifikasi Area yang diperhatikan

Kegiatan pada langkah empat adalah meninjau setiap kontainer untuk menentukan area yang menjadi perhatian selanjutnya membuat dokumentasi setiap area yang diperhatikan.

Langkah 5 – Mengidentifikasi Skenario Ancaman

Langkah 6 – Mengidentifikasi Risiko

Kegiatan pada langkah enam ini adalah mengidentifikasi niali dampak

Tabel 1 Identifikasi Nilai Dampak

Are Dampak	Prioritas	Nilai Dampak		
		Rendah (1)	Sedang (2)	Tinggi (3)
Reputasi dan Kepercayaan Pengguna	1	5	10	15
Keuangan	2	4	8	12
Produktifitas	3	3	6	9
Keselamatan dan Kesehatan Pegawai	4	2	4	6
Tuntutan Hukum	5	1	2	3

Langkah 7 – Menganalisis Risiko

Tabel 2 1 Allegro Worksheet 10-a

Allegro - Worksheet	**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	Aset Informasi	Data Penyedia Barang jasa		
	Area Perhatian	Eksploitasi celah keamanan sistem di server dari pihak luar		
Threat	(1) Actor	Tidak diketahui		
	(2) Means	Mengambil atau melakukan modifikasi data penyedia barang jasa		
	(3) Motive	Dengan sengaja		
	(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**		
	(5) Security Requirements	Meningkatkan keamanan software, hardware dan jaringan.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	**High**	**Medium**	✓ **Low**
	(7) Consequences	(8) Severity		
		Area	**Nil**	**Sc**
	Informasi yang dimodifikasi menyebabkan kerusakan mengganggu validitas informasi tersebut	**Terdampak**	**ai**	**ore**
		Reputasi dan Kepercaya	Tinggi	10
		Keuangan	Rendah	4
		Produktifitas	Tinggi	6
		Keselam	Re	2
		Tuntutan Hukum	Tinggi	3
			Relative Risk Score	**25**

Langkah 8 – Memilih Pendekatan Mitigasi

Tabel 3 Matriks Risiko Relatif

Risk Relative Matrix		
Risk Score	POOL	Mitigation Approach
30-45	1	Mitigasi
16-29	2	Defer
0-15	3	Accept

Berdasarkan pada tabel Risk Relative Matrix, maka pendekatan mitigasi akan ditentukan untuk tiap risiko. Jika nilai skor risiko antara 0 sampai 15 maka risiko tersebut bisa diterima. Nilai Skor antara 16 sampai 29 maka risiko tersebut dimitigasi atau bisa ditangguhkan. Jika nilai risiko antara 30 sampai 45 maka risiko tersebut harus dimitigasi.

Analisis Risiko OCTAVE Allegro –AHP

Setelah semua tahapan analisis OCTAVE Allegro dilakukan maka tahapan selanjutnya adalah menentukan peringkat area yang diperhatikan menggunakan metode AHP.

Tahap pertama adalah dengan membuat matrix inisiasi yang diambil dari nilai pada metode OCTAVE Allegro yaitu pada Worksheet 10. Hasil dari matrik inisiasi dapat dilihat pada tabel 4

Tabel 4 Tabel Inisiasi AHP

No	Area Perhatian (AP)	Reputasi	Keuangan	tas	an	Hukum	as
1	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam	10	4	6	2	3	8
2	Bocornya hak akses seperti username dan password administrator	10	4	9	2	3	4
3	Kesalahan ketika maintenance jaringan di ruang server	15	12	6	4	3	4
4	Gangguan koneksi internet	10	12	9	2	3	8
5	Kerusakan pada hardware server	10	12	9	2	2	8
6	Ruang server diakses oleh pihak tidak berwenang	15	4	3	2	3	4
7	Adanya bugs/error pada saat update sistem	15	4	3	2	3	12
8	Terhentinya layanan karena supply listrik mati	10	12	9	4	2	4
9	Bencana alam yang mengakibatkan kerusakan perangkat terkait	5	12	9	6	1	4

Tahap terakhir dari metode AHP membuat tabel peringkat area perhatian dengan memasukkan bobot dari nilai matriks yang didapatkan. Hasil peringkat risiko dapat dilihat pada tabel5.

Tabel 5 Peringkat Area Perhatian

No	Area Perhatian	Bobot	Rangking
1	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam	0,121674561	3
2	Bocornya hak akses seperti username dan password administrator	0,11536772	5
3	Kesalahan ketika maintenance jaringan di ruang server	0,085167708	7
4	Gangguan koneksi internet	0,121547747	4
5	Kerusakan pada hardware server	0,099824003	6
6	Ruang server diakses oleh pihak tidak berwenang	0,152596928	1
7	Adanya bugs/error pada saat update sistem	0,127790408	2
8	Terhentinya layanan karena supply listrik mati	0,083008283	8
9	Bencana alam yang mengakibatkan kerusakan perangkat terkait	0,080281282	9

Berdasarkan tabel peringkat area perhatian tersebut maka dapat ditentukan prioritas penanganan keamanan informasi dari yang memiliki risiko paling besar sampai dengan risiko paling rendah.

V. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan tersebut diatas, maka dapat dirumuskan beberapa simpulan sebagai berikut :

1. Metode OCTAVE Allegro dapat digunakan untuk melakukan analisis risiko keamanan informasi terhadap asset informasi yang dimiliki
2. Metode AHP dapat digunakan untuk menentukan peringkat risiko sehingga organisasi dapat menentukan prioritas dalam perencanaan mitigasi risiko.

REFERENCES

Badie, N., & Lashkari, A. H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. *J. Basic. Appl. Sci. Res*, *2*(9), 9331–9347. www.textroad.com

Caralli, R. a R. a. C., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. *Young*, *May*, 1–113.

Dorofee, A. (2005a). Managing Information Security Risks across the Enterprise. In *Guarding Your Business* (Issue April, pp. 151–172). https://doi.org/10.1007/0-306-48638-5_9

Dorofee, A. (2005b). Managing Information Security Risks across the Enterprise. In *Guarding Your Business* (pp. 151–172). Kluwer Academic Publishers. https://doi.org/10.1007/0-306-48638-5_9

Jufri, M. T., Hendayun, M., & Suharto, T. (2018). Risk-assessment based academic information System security policy using octave Allegro and ISO 27002. *Proceedings of the 2nd International Conference on Informatics and Computing, ICIC 2017*, *2018-Janua*, 1–6. https://doi.org/10.1109/IAC.2017.8280541

Keating, C. G. (2014). *Validating the Octave Allegro Information Systems Risk Assessment Methodology: A Case Study*. https://nsuworks.nova.edu/gscis_etd

Kuntari, N. L., Chrisnanto, Y. H., & ... (2018). Manajemen Risiko Sistem Informasi di Universitas Jenderal Achmad Yani Menggunakan Metoda Octave Allegro. *Seminar Nasional …*. http://prosiding.uika-bogor.ac.id/index.php/semnati/article/view/106/88

Magdalenić, I., Ivkovic, N., Maček, D., & Ivković, N. (n.d.). *Risk Assessment of the Bank's Noncompliance with Payment Card Industry Data Security Standard*. Retrieved May 22, 2021, from https://www.researchgate.net/publication/268369522

Matondang, N., Isnainiyah, I. N., & Muliawatic, A. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *2*(1), 282–287. https://doi.org/10.29207/resti.v2i1.96

Mazareanu, V. P. (2011). Risk Management and Analysis: Risk Assessment (Qualitative and Quantitative). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1549186

Munteanu, A. (2006). Information security risk assessment: The qualitative versus quantitative dilemma. *Managing Information in the Digital Economy: Issues and Solutions - Proceedings of the 6th International Business Information Management Association Conference, IBIMA 2006*, 227–232.

Prajanti, A. D., & Ramli, K. (2019, June 1). A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods. *34th International Technical Conference on Circuits/Systems, Computers and Communications, ITC-CSCC 2019*. https://doi.org/10.1109/ITC-CSCC.2019.8793421

Rahardjo, B. (1998). *Keamanan Sistem Informasi Berbasis Internet*.

RI, K. S. (2020). Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. *Menteri Hukum Dan Hak Asasi Manusia Republik Indonesia*, 110.

Riasetiawan, M. (2016). Pusat Data untuk Pemerintahan. *Departemen Ilmu Komputer Dan Elektronik, FMIPA*

UGM, 1–57. http://mardhani.staff.ugm.ac.id/files/2016/03/Pusat-Data-untuk-Pemerintahan.pdf

Saaty, R. W. (1987). The analytic hierarchy process-what it is and how it is used. *Mathematical Modelling*, *9*(3–5), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8

Sardjono, W., & Cholik, M. I. (2018). Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank. *Proceedings of 2018 International Conference on Information Management and Technology, ICIMTech 2018*, 38–42. https://doi.org/10.1109/ICIMTech.2018.8528108

St, R. F., Adhitya, R., & St, N. (2020). *Analisis Risiko Keamanan Informasi Menggunakan Metode Octave Allegro Pada Dinas Komunikasi Dan Informatika*. *7*(2), 7003–7008.

Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment of Information System Risk Management with Octave Allegro at Education Institution. *Procedia Computer Science*, *135*, 202–213. https://doi.org/10.1016/j.procs.2018.08.167

Thibadeau, B. (2007). Prioritizing project risks using AHP. *PMI Global Congress 2007*, 1–9. https://www.pmi.org/learning/library/project-decision-making-tool-7292