ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO PADA DINAS KOMUNIKASI DAN INFORMATIKA JAWA BARAT

1*Greenhard Sitorus
Information System
Telkom University
Bandung, Indonesia
greenhardsi@gmail.com

2*Rokhman Fauzi ST., M.T.
Information System
Telkom University
Bandung, Indonesia
rokhmanfauzi@telkomuniversity.ac.id

3*Ryan Adhitya Nugraha ST., M.T.
Information System
Telkom University
Bandung, Indonesia
ranugraha@telkomuniversity.ac.id

***Abstrak*— Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi suatu kebutuhan dan tututan bagi setiap instansi peyelenggara pelayanan publik, mengingat peran TIK yang semakin penting bagi upaya peningkatan kualitas sebagai salah satu realisasi dari tata kelola pemerintah yang baik. Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting untuk diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan, keutuhan, dan ketersediaan.**

Teknologi informasi juga kini telah menjadi hal yang sangat penting karena sudah banyak instansi pemerintah yang menggunakan teknologi informasi sebagai alat yang mendukung dalam menjaga dan meningkatkan kualitas informasinya. Seperti halnya teknologi informasi yang dirangkai menjadi suatu kesatuan sistem informasi yang dapat menjadi penunjang utama dalam proses pengelolaan data untuk menghasilkan informasi yang dapat dicerna serta dipahami dengan baik dan jelas.

Dalam menerapkan tata kelola teknologi informasi terkadang muncul berbagai risiko serta ancaman yang tak terduga yang dapat mengganggu keberlangsungan sistem informasi sehingga dapat mengakibatkan kerugian bagi instansi pemerintah tersebut.

Maka dari itu diperlukan adanya suatu penilaian risiko yang dapat membuat manajemen keamanan informasi pada instansi pemerintah tersebut menjadi lebih efektif, efisien dan berkesinambungan. Serta penilaian risiko tersebut dapat menjadi pendoman untuk menerapkan kebijakan yang belum dijalankan dengan semestinya, dan menjadi pembanding terhadap terhadap kebijakan yang sudah diterapkan. Untuk dalam penelitian ini dilakukan penilaian risiko terhadap kerentanan informasi.

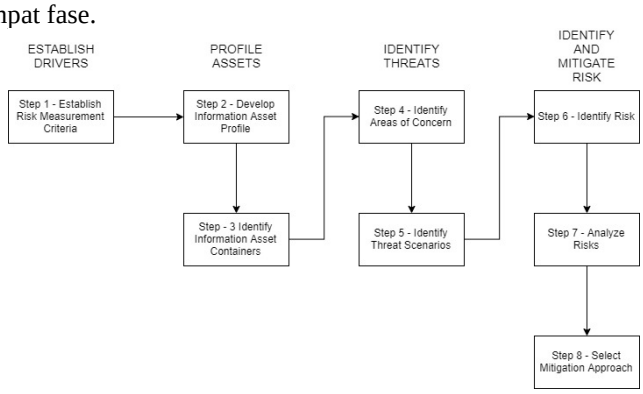
***Kata Kunci*— Teknologi Informasi dan Komunikasi, Sistem Informasi, Tata Kelola Teknologi Informasi, Penilaian Risiko, OCTAVE, OCTAVE Allegro.**

I. PENDAHULUAN

Penelitian ini memfokuskan pada analisis, identifikasi, dan penilaian risiko keamanan teknologi informasi pada aset teknologi informasi di Dinas Komunikasi dan Informatika Jawa Barat menggunakan metode OCTAVE Allegro, serta hasil dari pada penilaian risiko tersebut akan menjadi acuan dalam mengusulkan kebijakan yang dianggap sesuai dengan keadaan di Dinas Komunikasi dan Informatika Jawa Barat saat ini.

II. METODOLOGI PENELITIAN OCTAVE ALLEGRO

OCTAVE Allegro merupakan metode yang disederhanakan dengan fokus pada aset informasi. OCTAVE Allegro dapat dilakukan dengan metode workshopstyle dan kolaboratif. OCTAVE Allegro terdiri dari delapan langkah dibagi dalam empat fase.



Gbr 1. Langkah – Langkah OCTAVE Allegro

III. DISKOMINFO

Pada bab ini menjelaskan tentang visi – misi diskominfo dan juga menjelaskan tentang aplikasi yang menjadi objek penelitian pada kali ini yaitu aplikasi Service Desk.

A. VISI MISI

Visi Diskominfo Jabar adalah Terwujudnya Masyarakat Informasi Jawa Barat Melalui Penyelenggaran Komunikasi dan Informatika yang Efektif dan Efisien.

Misi Diskominfo Jabar adalah 1. Meningkatkan sarana prasarana dan profesionalisme sumberdaya aparatur bidang komunikasi dan informatika, mengoptimalkan pengelolaan pos dan telekomunikasi, mengoptimalkan pemanfaatan sarana komunikasi dan informasi pemerintah dan masyarakat, serta melaksanakan diseminasi informasi, mewujudkan layanan online dalam penyelenggaraan pemerintahan berbasisi teknologi informasi dan komunikasi dan mewujudkan pengelolaan data menuju satu data pembangunan untuk Jawa barat.

B. SERVICE DESK

Service Desk merupakan aplikasi berbasis website yang digunakan untuk memfasilitasi perangkat daerah dalam melakukan permintaan atau keluhan terhadap penerapan layanan teknologi informasi dilingkungan Pemerintah Provinsi Jawa Barat secara terpadu dan terpusat dalam satu

portal. Transaksi yang ada pada servicedesk ini mengadopsi penerapan ITIL (Information Technology Infrastructure Library) menggunakan CMDB (Configuration Management Data Base) sebagai proses inti operasional, untuk tiket serta turunannya yaitu request permintaan dan laporan insiden. Servicedesk dapat digunakan oleh tim IT atau tingkatan manajemen dan terintegrasi dengan perangkat TI lainnya (sistem pemantauan, alat pelaporan, inventarisasi otomatis, dll).

IV. LANGKAH DAN ANALISIS

Pada bagian ini akan dijelaskan, Langkah – Langkah kerja dari OCTAVE Allegro, berikut ini merupakan beberapa contoh hasil kerja menggunakan metode OCTAVE Allegro.

A. LANGKAH 1, MEMBANGUN KRITERIA PENGUKURAN RISIKO

Langkah ini terdapat dua aktivitas, diawali dengan membangun organizational drivers digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting. Aktivitas dua yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada risk measurement criteria worksheets. Aktivitas dua melakukan pemberian nilai prioritas impact area menggunakan impact area ranking worksheet.

TABEL I
HASIL MEMBANGUN KRITERIA PENGUKURAN RISIKO

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA - REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	Low	Medium	High
Reputation (Reputasi)	Berpengaruh kecil terhadap reputasi dan dibutuhkan usaha minimal untuk memperbaiki-nya	Berpengaruh sedang terhadap reputasi dan dibutuhkan usaha yang cukup untuk memperbaiki-nya	Berpengaruh besar terhadap reputasi dan dibutuhkan usaha yang besar untuk memperbaiki-nya
Customer Loss (kerugian pelanggan)	Kurang dari 2% pengurangan pelanggan akibat kehilangan kepercayaan	2% sampai 10% pengurangan pelanggan akibat kehilangan kepercayaan	Lebih dari 10% pengurangan pelanggan akibat kehilangan kepercayaan

B. LANGKAH 2, MENGEMBANGKAN PROFIL ASET INFORMASI

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai informasi aset yang penting, dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi aset informasi kritis kemudian mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk confidentiality, integrity dan availaibility. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

TABEL II
HASIL MENGEMBANGKAN PROFIL ASET INFORMASI

Allegro Worksheet 8a	CRITICAL INFORMATION ASSET PROFILE	
Critical Asset	Rationale for Selection	Description
What is the critical information asset?	*Why is this information asset important to the organization?*	*What is the agreed-upon description of this information asset?*
Data User	Karena pegawai yang melakukan permintaan atau membuat tiket baru harus diketahui agar diketahui letak problem dan alasan tiket dibuat	Berisi tentang nama pegawai, NIP, bidang dan dari perangkat daerah mana, serta username, dan password
Owner(s)		
Bidang E-gov/Pengelolaan Diskominfo Jawa Barat		
Security Requirements		
What are the security requirements for this information asset?		
Confidentiality	Only authorized personnel can view this information asset, as follows:	Admin
Integrity	Only authorized personnel can modify this information asset, as follows:	Caller, Helpdesk, Admin
Availability	This asset must be available for these personnel to do their jobs, as follows	Caller, Helpdesk, Admin
	This asset must be available for 24 hours, 7 days/week.	
Most Important Security Requirement		
What is the most important security requirement for this information asset?		
[] Confidentiality	[v] Integrity	[] Availability

C. LANGKAH 3, MENGIDENTIFIKASI KONTAINER DAN ASET INFORMASI

Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi dilindung, tingkat perlindungan atau pengaman aset informasi dan

kerentanan serta ancaman terhadap kontainer dari aset informasi.

TABEL III
HASIL MENGIDENTIFIKASI KONTAINER DAN ASET INFORMASI (TEKNIKAL)

Allegro Worksheet 9a - Data User	INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1. Database: Data Pegawai Data disimpan pada database Service Desk yang berada di DISKOMINFO JABAR	Bidang e-Gov DISKOMINFO JABAR
2. Aplikasi: Service Desk Data diakses menggunakan aplikasi Service Desk yang dimiliki oleh DISKOMINFO JABAR	Bidang e-Gov DISKOMINFO JABAR
3. Perangkat Keras Perangkat yang digunakan untuk mengakses portal Service Desk adalah Komputer dengan jaringan internet dan LAN	Bidang e-Gov DISKOMINFO JABAR
EXTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1. Aplikasi: Service Desk Data diakses menggunakan aplikasi Service Desk yang dapat digunakan Dinas terkait	Dinas terkait
2. Perangkat Keras Perangkat yang digunakan untuk mengakses portal Service Desk adalah Komputer dengan jaringan internet dan LAN	Dinas terkait

TABELIV
HASIL MENGIDENTIFIKASI KONTAINER DAN ASET INFORMASI (TEKNIKAL)

Allegro Worksheet 9b – Data User	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1. Form Registrasi Pegawai Form registrasi pegawai yang diinputkan berdasarkan data pegawai yang ada pada suatu dinas terkait atau pun DISKOMINFO JABAR sendiri	Bidang e-Gov DISKOMINFO JABAR
EXTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1. Form Registrasi Pegawai Form registrasi pegawai yang harus dilengkapi agar nanti dapat diberikan kepada DISKOMINFO JABAR untuk validasi	Dinas terkait

TABEL V
HASIL MENGIDENTIFIKASI KONTAINER DAN ASET INFORMASI (PEOPLE)

Allegro Worksheet 9c - Data User	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
Helpdesk	Bidang e-Gov DISKOMINFO JABAR
Admin	Bidang e-Gov DISKOMINFO JABAR
Teknisi	Bidang e-Gov DISKOMINFO JABAR
Caller	Bidang e-Gov DISKOMINFO JABAR
EXTERNAL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
Admin	Dinas/Bidang terkait
Caller	Dinas/Bidang terkait

D. LANGKAH 4, MENGIDENTIFIKASI AREA MASALAH

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi. Dengan berpedoman pada dokumen information asset risk environment maps dan information asset risk worksheet maka dapat dicatat area of concern. Berpedoman pada dokumen information asset risk worksheet lakukan review dari kontainer untuk membuat area of concern dan mendokumentasikan setiap area of concern.

TABEL VI
HASIL MENGIDENTIFIKASI AREA MASALAH PADA DATA USER

No.	Area Of Concern - Data User
1	Pemanfaatan celah keamanan sistem informasi oleh pihak luar maupun pihak dalam
2	Penyebaran hak akses terhadap data user
3	Kehilangan data user karena tidak melakukan backup data
4	Kesalahan dalam menginput data user
5	Kerusakan pada data user
6	Kebocoran data user
7	Pemalsuan data terhadap data user

E. LANGKAH 5, MENGIDENTIFIKASI SKENARIO ANCAMAN

Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan appendix cthreat scenarios questionnaries. Aktivitas dua melengkapi information asset risk worksheets untuk setiap threat scenario yang umum.

TABEL VII
HASIL MENGIDENTIFIKASI SALAH SATU SKENARIO ANCAMAN PADA DATA USER

Information Asset	Data User
Area of Concern	Pemanfaatan celah keamanan sistem informasi oleh pihak luar maupun pihak dalam
1- Actor	Tidak Diketahui
2 - Means	Pemanfaatan celah keamanan dari server, database atau Modul oleh pihak luar maupun dalam
3 - Motives	Dengan sengaja
4 - Outcome	[v] Disclosure [v] Modification [v] Destruction [v] Interuption
5 - Security Requirement	Meningkatkan keamanan software, hardware, dan jaringan. Dilakukan pemantauan berkala terhadap keamanan sistem

F. LANGKAH 6, MENGIDENTIFIKASI RISIKO

Aktivitas satu pada langkah enam menentukan threat scenario yang telah didokumentasikan di information asset risk worksheet dapat memberikan dampak bagi organisasi.

TABEL VIII
HASIL MENGIDENTIFIKASI RISIKO

Area of Concern	Pemanfaatan celah keamanan sistem informasi oleh pihak luar maupun pihak dalam
6- Consequences	
Informasi yang dapat dimodifikasi karena adanya celah keamanan dapat menyebabkan informasi tersebut tidak utuh maupun rusak sehingga mengganggu system informasi yang sedang berjalan.	

G. LANGKAH 7, MENGANALISA RISIKO

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada information asset risk worksheet. Aktivitas satu dimulai dengan melakukan review risk measurement criteria dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

TABEL IX
PRIORITAS IMPACT AREA

Impact Areas	*Priority*	*Low* (1)	*Medium* (2)	*High* (3)
Reputation and Customer Confidence	2	2	4	6
Financial	4	4	8	12
Productivity	5	5	10	15
Safety and Health	1	1	2	3
Fines and Lawsuits	3	3	6	9

Priority yang memiliki prioritas paling penting hingga terendah diurutkan berdasarkan value Priority nya adalah 5,4,3,2,1. Langkah 4 hingga dengan langkah ke 7 ini dikerjakan menggunakan worksheet 10 OCTAVE Allegro.

TABEL X
PENILAIIAN RISIKO

Allegro - Worksheet 10a	INFORMATION ASSET RISK WORKSHEET		
Threat	Information Asset	Data User	
	Area of Concern	Pemanfaatan celah keamanan sistem informasi oleh pihak luar maupun pihak dalam	
	1- Actor	Tidak Diketahui	
	2 - Means	Pemanfaatan celah keamanan dari server, database atau Modul oleh pihak luar maupun dalam	
	3 - Motives	Dengan sengaja	
	4 - Outcome	[v] Disclosure [v] Modification [v] Destruction [v] Interuption	
	5 - Security Requirement	Meningkatkan keamanan *software*, *hardware*, dan jaringan. Dilakukan pemantauan berkala terhadap keamanan sistem	
6 - Consequnces	7 - Severity		
Informasi yang dapat dimodifikasi karena adanya celah keamanan dapat menyebabkan informasi tersebut tidak utuh maupun rusak sehingga mengganggu system informasi yang sedang berjalan.	Impact Area	Value	Score
	Reputation & Customer Confidence	Medium	4
	Financial	Medium	8
	Productivity	High	15
	Safety & Health	Low	1
	Fines & Legal Penalties	Medium	9
Relative Risk Score			37

H. LANGKAH 8, MEMILIH PENDEKATAN MITIGASI

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasaarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

TABEL XI
RISK RELATIVE MATRIX

Risk Relative Matrix		
Risk Score	POOL	Mitigation Approach
30-45	1	Mitigate

16-29	2	Defer
0-15	3	Accept

(TAHER J, HENDAYUN, & SUHARTO, 2017)

Berdasarkan Risk Relative Matrix, maka pendekatan mitigasi akan ditentukan untuk tiap risiko, berikut ini hasil akhirnya.

TABEL XII
HASIL ANALISIS RISIKO

Area of Concern	***Action***
Kerusakan pada data user	*Mitigate*
Kebocoran data user	*Mitigate*
Pemalsuan data terhadap data user	*Mitigate*
Pemanfaatan celah keamanan sistem informasi oleh pihak luar maupun pihak dalam – data permintaan layan	*Mitigate*
Penyebaran hak akses terhadap data permintaan layanan	*Defer*
Kehilangan data permintaan layanan karena tidak melakukan backup data	*Mitigate*
Kesalahan dalam menginput data permintaan layanan	*Accept*
Kerusakan pada data permintaan layanan	*Mitigate*
Kebocoran data permintaan layanan	*Mitigate*
Pemanfaatan celah keamanan sistem informasi oleh pihak luar maupun pihak dalam – data permintaan diproses	*Mitigate*
Penyebaran hak akses terhadap data permintaan layanan yang sedang diproses	*Defer*
Kehilangan data permintaan layanan yang sedang diproses karena tidak melakukan backup data	*Mitigate*
Kesalahan dalam menginput data permintaan layanan yang sedang diproses	*Accept*
Kerusakan pada data permintaan layanan yang sedang diproses	*Mitigate*
Kebocoran data permintaan layanan yang sedang diproses	*Mitigate*
Pemanfaatan celah keamanan sistem informasi oleh pihak luar maupun pihak dalam – data tiket	*Mitigate*
Penyebaran hak akses terhadap data tiket	*Defer*
Kehilangan data tiket karena tidak melakukan backup data	*Mitigate*
Kesalahan dalam menginput data tiket	*Accept*
Kerusakan pada data tiket	*Mitigate*
Kebocoran data tiket	*Mitigate*
Pemanfaatan celah keamanan sistem informasi oleh pihak luar maupun pihak dalam – data insiden	*Mitigate*
Penyebaran hak akses terhadap data insiden	*Defer*
Kehilangan data insiden karena tidak melakukan backup data	*Mitigate*
Kesalahan dalam menginput data insiden	*Accept*
Kerusakan pada data insiden	*Mitigate*
Kebocoran data insiden	*Mitigate*
Pemanfaatan celah keamanan sistem informasi oleh pihak luar maupun pihak dalam – data layanan	*Mitigate*
Penyebaran hak akses terhadap data layanan	*Defer*
Kehilangan data layanan karena tidak melakukan backup data	*Mitigate*
Kesalahan dalam menginput data layanan	*Accept*
Kerusakan pada data layanan	*Mitigate*
Kebocoran data layanan	*Mitigate*

V. REKOMENDASI KEBIJAKAN

Pada metode OCTAVE Allegro tidak ada panduan yang digunakan dalam mengontrol risiko maka dari pada itu digunakan ISO 27001 sebagai acuan dalam memberikan kontrol untuk risiko. Pada bab ini berisikan tentang rekomendasi kontrol menggunkan ISO 27001 dari risiko-risiko yang sudah diindenfikasi sebelumnya, rekomendasi ini disesuaikan dengan kebutuhan dan keadaan dari risiko tersebut.

Kebijakan merupakan suatu rangkaian pedoman dan dasar rencana dalam melakukan suatu pekerjaan serta menjadi panduan dalam menangani risiko yang dapat menyerang aset informasi kritis yang sudah diidentifikasi sebelumnya. Perancangan dan rekomendasi yang dilakukan yaitu berdasarkan hasil dari analisis risiko menggunakan metode OCTAVE Allegro dan analisis kontrol risiko menggunakan panduan ISO 27001. Tabel dibawah ini menjelaskan tentang pengelompokan untuk menentukan rekomendasi kebijakan yang diambil berdasarkan risiko yang sudah dianalisis.

TABEL XII
CONTOH HASIL KEBIJAKAN YANG DISIMPULKAN

Kebijakan Kebijakan Kriptografi
Referensi 1. Peraturan Kepala Lembaga Sandi Negara Nomor 5 Tahun 2014 tentang Standar Algoritma Kriptografi pada Instansi Pemerintah 2. ISO 27001
Pernyataan 1. Organisasi mengklasifikasikan tingkat keamanan yang digunakan. 2. Organisasi melakukan evaluasi terhadap Standar Algoritma Kriptografi pada Instansi Pemerintah paling sedikit satu kali dalam lima tahun. 3. Organisasi melakukan pengembangan Standar Algoritma Kriptografi disesuaikan dengan kebutuhan. 4. Organisasi harus melaporkan kepada Lembaga Sandi Negara apabila terjadi permasalahan dalam penggunaan Algoritma Kriptografi.

VI. KESIMPULAN DAN SARAN

Pada bab ini menjelaskan tentang kesimpulan dari penelitian dan analisis yang sudah dilakukan dari penelitian ini dan saran- saran untuk objek penelitian dan bagi peneliti berikutnya berdasarkan hasil penelitian.

A. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan pada aplikasi Service Desk milih Dinas Komunikasi dan Informatika Jawa Barat yang dikelola oleh bagian e-Government menggunakan metode OCTAVE Allegro maka dapat disimpulkan:

1. Aplikasi Service Desk memiliki 6 aset informasi kritis, yaitu data User, data Permintaan Layanan, data Permintaan Diproses, data Tiket, data Insiden, dan data Layanan.
2. Dengan menggunakan metode OCTAVE Allegro dapat diidentifikasi 5 impact areas penting yang menjadi indikator dalam penilaian dan mitigasi risiko yang

nantinya akan digunakan, yaitu Reputation and Customer Confidence, Financial, Productivity, Safety and Health, dan Fines and Legal Penalties.

3. Risiko yang teridentifikasi adalah sebanyak 37 area, risiko akan diidenfikasi profil dan konsekuensinya. Setelah itu risiko akan dinilai menggunakan indikator impact areas dan ditentukan POOLnya berdasarkan Risk Relative Matrix yang sudah ditetapkan, gunanya adalah untuk menentukan pendekatan mitigasi yang akan digunakan pada suatu risiko. Hasil analisis menunjukan 25 risiko akan dimitigasi (mitigate), 6 akan ditangguhkan (defer), dan 6 lagi akan diterima(accept).
4. Rekomendasi kebijakan dibuat menggunakan kontrol ISO 27001 untuk melihat bagaimana cara untuk menentukan kebijakan yang sesuai dengan hasil analisis risiko sebelumnya.
5. Prosedur dibuat berdasarkan hasil analisis risiko dan rekomendasi kebijakan.

B. SARAN

Adapun saran dari penelitian ini untuk Dinas Komunikasi dan Informatika Jawa Barat dan peneliti selanjutnya adalah:

1. Dapat menjadikan hasil analisis risiko ini menjadi salah satu referensi bahwa setiap aset informasi pasti memiliki potensi riisko.
2. Dapat menjadikan hasil analisis risiko ini menjadi salah satu referensi dalam menetapkan dan menganalisis risiko aset informasi.
3. Organisasi dapat menggunakan suatu guideline, standard dan atau framework dalam melakukan analisis risiko, seperti OCTAVE Allegro dan ISO 27001.
4. Peneliti selanjutnya dapat mengkomparasi hasil analisis dengan menggunakan metode lain yang berkaitan dengan aplikasi Service Desk.

REFERENSI

[1] Alberts, C., & Dorofee, A. (2002). Managing Information Security Risks: The OCTAVE Approach. Boston: Addison Wesley.

[2] Angraini, Megawati, & Haris, L. (2018). Risk Assessment on Information Asset an academic Application Using ISO 27001. 2018 6th International Conference on Cyber and IT Service Management (CITSM), 1-6.

[3] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Pittsburgh: Software Engineering Institute Carnegie Mellon University.

[4] Chung, H., Cho, S. P., & Jang, Y. (2014). Standardizations on IT risk analysis service in NGN. 16th International Conference on Advanced Communication Technology, 1-4.

[5] Djohanputro, B. (2008). Manajemen Risiko Korporat. Jakarta: PPM Manajemen.

[6] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science In Information Systems Research. South Florida: MIS Quarterly.

[7] Iksan, H., & Jarti, N. (2018). Analisis Risiko Keamanan Teknologi Informasi Menggunakan OCTAVE Allegro. Jurnal Responsive Teknik Informatika, Sekolah Tinggi Teknik Ibnu Sina, 1-11.

[8] International Standard. (2009). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. Geneva: ISO.

[9] International Standard. (2011). ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. Geneva: ISO.

[10] Jufri, M. T., Hendayun, M., & Suharto, T. (2017). Risk-Assessment Based Academic Information System Security Policy Using OCTAVE Allegro and ISO 27002. Second International Conference on Informatics and Computing (ICIC), 1-6.

[11] KEMKOMINFO. (2011). Panduan Penerapan Tata Kelola Informasi Bagi Penyelenggara Pelayanan Publik. Jakarta: Kementrian Komunikasi dan Informatika RI.

[12] Kunantari, N. L., Chrisnanto, Y. H., & Hadiana, A. I. (2018). Manajemen Risiko Sistem Informasi Di Universitas Jendral Achmad Yani Menggunakan Metoda OCTAVE Allegro. Seminar Nasional Teknologi Informasi Universitas Ibn Khaldun Bogor, 1-9.

[13] Matondang, N., Isnainiyah, I. N., & Muliawati, A. (2018). Analisis Manajemen Risiko Data Keamanan Informasi (Studi Kasus: RSUD XYZ). Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 282-287.

[14] Prajanti, A. D., & Ramli, K. (2019). 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), 1-4.

[15] Sardjono, W., & Cholik, M. I. (2018). Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank. International Conference on Information Management and Technology (ICIMTech), 1-5.

[16] Suroso, J. S., Rahaju, S. M., & Kusnadi. (2018). Evaluation Of IS Risk Management Using Octave Allegro In Education Division. International Conference on Orange Technologies (ICOT), 1-3.

[17] Taher J, M., Hendayun, M., & Suharto, T. (2017). Risk-Assessment Based Academic Information System Security Policy Using OCTAVE Allegro and ISO 27002. 2017 Second International Conference on Informatics and Computing (ICIC) (pp. 1-6). Jayapura: IEEE.

[18] Tjirare, D. J., & Shava, F. B. (2017). A gap analysis of the ISO/IEC 27000 standard implementation in Namibia. IST-Africa Week Conference (IST-Africa), 1-10.