Jurnal Teknik Elektro dan Komputasi (ELKOM)
Volume 6 Nomor 2 Agustus 2024 ‖ Hal. 255-261
ISSN : 2685-1814 (*Print*)
ISSN : 2685-7677 (*Online*)

Analisis dan Pengelolaan Risiko Keamanan Informasi Puskesmas Menggunakan Metode *Octave Allegro* (Studi Kasus: Puskesmas XYZ)

Dian Saputra[1*], M. Said Hasibuan[1]
[1]Fakultas Teknik Informatika, Institut Informatika & Bisnis Darmajaya
Jl. ZA. Pagaralam, Bandar Lampung
E-mail: diansa.2121210026@mail.darmajaya.ac.id

Naskah Masuk: 18 Juni 2023; Diterima: 11 Agustus 2024; Terbit: 31 Agustus 2024

ABSTRAK

Abstrak - Keamanan data dan informasi sangat penting untuk diterapkan bagi organisasi dan perusahaan, sebab tujuan dari keamanan informasi adalah menjaga integritas, kerahasiaan serta ketersediaan di organisasi atau perusahaan tersebut untuk mencapai Tata Kelola teknologi informasi yang baik. Ketika tidak diperlakukan dengan tepat dan benar, maka akan berdampak buruk bagi organisasi atau perusahaan tersebut yang mengarah pada masalah dan peringatan yang tidak disangka. Saat ini penelitian pada Puskesmas XYZ bertujuan untuk menganalisis dan mengklarifikasi keamanan Sistem Informasi. Puskesmas XYZ dalam dalam hal ini tidak pernah mengukur risiko dan tidak menerapkan manajemen risiko serta keamanan informasi secara terorganisir, sehingga data pada Puskesmas XYZ sering diretas. Untuk mengatasi masalah tersebut pada Puskesmas XYZ digunakan metode *octave allegro* yang berfungsi mengontrol serta membantu karyawannya mengerti arti dari informasi yang dimaksud, berikut ancaman serta risiko yang akan terjadi. sehingga pengelolaan keamanan informasi menjadi baik, efektif dan efisien. Oleh karena itu, untuk meminimalkan banyak kemungkinan risiko Puskesmas XYZ perlu mengukur keamanan informasi. Dengan hadirnya metode tersebut dapat diterapkan pada Puskesmas XYZ untuk mengukur resiko keamanan dan menjadikan manajemen resiko terstruktur secara sistem. Diharapkan pentingnya manajemen risiko mendapat pedoman untuk perbaikan implementasi keamanan informasi dan mencari solusi atas risiko umum yang terjadi pada Puskesmas XYZ. Ruang lingkup akan diselidiki dan fokus hanya pada metode, proses dan kegiatan yang ada di Puskesmas XYZ untuk mempertahankan pengetahuan tentang risiko yang muncul. Penilaian yang dilakukan di Puskesmas XYZ mencakup 8 area mencakup uji data, infrastruktur, aplikasi, hardware, software, internet serta personel.

Kata kunci: Keamanan Informasi, Manajamen Risiko, *Octave allegro*, Puskesmas XYZ

ABSTRACT

Abstract *- Data and information security is very important to implement for organizations and companies, because the purpose of information security is to maintain integrity, confidentiality and availability in the organization or company to achieve good information technology governance. When not treated properly and correctly, it will have a bad impact on the organization or company which leads to unexpected problems and warnings. Currently research at the XYZ Health Center aims to analyze and clarify information system security. XYZ Health Center in this case never measures risk and does not implement risk management and information security in an organized manner, so that data at XYZ Health Center is often hacked. To overcome this problem at the XYZ Health Center the octave allegro method is used which functions to control and help employees understand the meaning of the information in question, along with the threats and risks that will occur. So that information security management is good, effective and efficient. Therefore, to minimize the many possible risks, the XYZ Health Center needs to measure information security. With the presence of this method, it can be applied to the XYZ Health Center to measure security risks and make risk management structured in a systemic way. It is hoped that it is important for risk management to receive guidelines for improving the implementation of information security and finding solutions to common risks that occur at the XYZ Health Center. The scope will be investigated and focus only on existing methods, processes and activities in Puskesmas XYZ to maintain knowledge about emerging risks. The assessment carried out at the XYZ Health Center covered 8 areas including testing data, infrastructure, applications, hardware, software, internet and personnel.*

Keyword: *Information Security, Risk Management, Octave allegro, Health Center XYZ*

1. PENDAHULUAN

Menerapkan manajemen risiko dan mengukur risiko keamanan saat ini dapat mengakomodasi organisasi mengembangkan praktik pencegahan ancaman sekaligus memberi perlindungan bagi organisasi beserta ancaman keamanannya [1]. Ada beberapa risiko yang dilaksanakan oleh Puskesmas dihadapkan

pada pengukuran risiko atau nilai risiko. Puskesmas XYZ, didirikan pada tahun 2015, dengan akreditasi B dibawah naungan Pemerintah. Saat ini, manajemen risiko belum diterapkan dalam pengelolaan proses bisnis Puskesmas XYZ dengan pengukuran risiko. Sebelumnya Puskesmas XYZ menerapkan manajemen resiko dengan melakukan penerapan secara tertulis, jadi apa yang menjadi tolok ukur belum dapat disimpulkan secara terstruktur. Oleh karena itu, untuk meminimalkan banyak kemungkinan risiko Puskesmas XYZ perlu mengukur keamanan informasi. Dengan hadirnya metode tersebut dapat diterapkan pada Puskesmas XYZ untuk mengukur resiko keamanan dan menjadikan manajemen resiko terstruktur secara sistem.

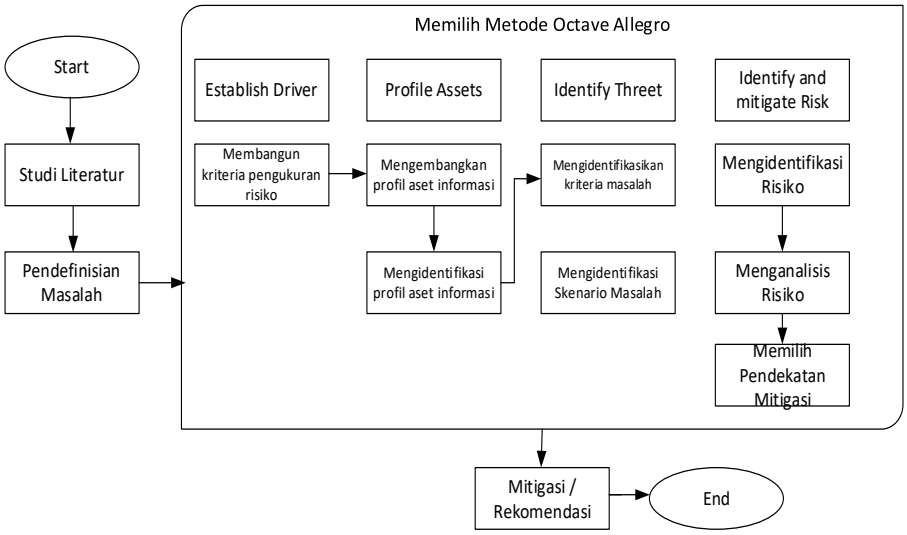
Diharapkan pentingnya manajemen risiko mendapat pedoman untuk perbaikan implementasi keamanan informasi dan mencari solusi atas risiko umum yang terjadi pada Puskesmas XYZ [2]. Ruang lingkup akan diselidiki dan fokus hanya pada metode, proses dan kegiatan yang ada di Puskesmas XYZ untuk mempertahankan pengetahuan tentang risiko yang muncul. itu bisa terjadi. Penilaian yang dilakukan di Puskesmas XYZ mencakup 8 area mencakup uji data, infrastruktur, aplikasi, *hardware*, *software*, internet serta personel.

Dalam hal ini Puskesmas XYZ untuk mencapai target area tersebut juga diperlukan sumber daya manusia yang bisa untuk membidangi hal tersebut, sehingga apa yang diharapkan dapat dicapai sesuai target yang di inginkan. Dengan hadirnya metode yang digunakan akan dapat mempermudah manajemen dalam mengelola teknologi informasi yang berkaitan dengan keamanan informasi sehingga tata kelola teknologi informasi menjadi baik, efektif dan efisien.

2. METODE PENELITIAN

2.1. Tahap Penelitian

Penelitian di Puskesmas XYZ diawali dengan kajian pustaka, kemudian merumuskan atau mengidentifikasi masalah yang terkait dengan potensi risiko keamanan informasi Puskesmas XYZ. Setelah dirumuskan masalahnya, selanjutnya dianalisis menggunakan metode *Octave allegro* [3] [4]. Berikutnya memeriksa data yang diperoleh sebagian melalui proses penelitian lapangan Staf Puskesmas XYZ. Tujuan dari pengumpulan data yaitu untuk mencari informasi yang diperlukan untuk mengidentifikasi risiko keamanan informasi agar proses riset berjalan optimal. Berdasarkan hasil studi metode *Octave allegro*, ditawarkan berbagai solusi dan rekomendasi memperkecil masalah ini. Terdapat beberapa tahapan penelitian yang dilaksanakan pada Puskesmas XYZ, tahapan kajian ini dapat dilihat sebagai berikut:



Gambar 1. Tahapan penelitian

Dalam tahapan ini metode *Octave allegro* memberikan solusi untuk mengidentifikasi resiko keamanan informasi yang dapat di persingkat melalui sistem sehingga menjadi lebih efektif dan esisien.

2.2. Pengumpulan Data

Mempelajari literatur menjadi tujuan penting penelitian karena dapat dianggap sebagai proses penelitian pertama. Penelitian kepustakaan yaitu dengan kegiatan membaca, menulis, dan mengolah data pustaka yang dipakai sebagai bahan penelitian [5]. Teknik pencarian literatur digunakan untuk mencari beberapa teori terkait yang dapat mendukung penelitian yang dilakukan.

2.3. Definisi Masalah

Mendefinisikan masalah membantu peneliti memberikan tujuan penelitian. Rekomendasi sesuai dengan kemungkinan masalah yang dapat didasarkan pada tinjauan pustaka menjelaskan bahwa Puskesmas XYZ belum memiliki aplikasi pengukuran dan manajemen risiko. [6] Oleh karena itu diperlukan manajemen risiko keamanan informasi yang dapat membantu Puskesmas XYZ mengurangi dan mengantisipasi ancaman yang mungkin muncul di masa mendatang.

2.4. Rekomendasi atau Mitigasi

Hasil penelitian ini berupa rencana perbaikan atau rekomendasi yang dapat dijadikan pedoman atau saran. Implementasi manajemen risiko keamanan informasi yang dapat membantu Puskesmas XYZ untuk mengurangi dan mengantisipasi ancaman di masa depan.

3. HASIL DAN PEMBAHASAN

Octave, juga dikenal sebagai *Operationally Critical Threat, Asset, and Vulnerability Evaluation* merupakan rangkaian komponen yang komprehensif dan sistematis dalam penilaian risiko keamanan informasi berbasis konteks. Metode *octave allegro* dirancang untuk memungkinkan penilaian risiko yang luas dengan tujuan menghasilkan hasil yang lebih akurat tanpa perlu pengetahuan mendalam tentang penilaian risiko. Untuk mengidentifikasi masalah yang terjadi pada Puskesmas XYZ maka di gunakan metode ini sebagai penggerak organisasi yang berfungsi untuk bahan evaluasi dari dampak risiko tujuan bisnis, mengidentifikasi area masalah, mengidentifikasi skenario ancaman, menganalisis risiko serta mengembangkan profil asset informasi.

3.1. Kriteria Pengukuran Risiko

Berdasarkan tahap analisis faktor kriteria pengukuran risiko menentukan area dampak dan memberikan skala besar untuk bidang pengaruh yang ditemukan. Identifikasi *driver* organisasi digunakan untuk menilai dampak setiap area [7] pada tabel kriteria pengukuran risiko diprioritaskan berdasarkan risiko yang ada. Menganalisis hasil dari kriteria pengukuran risiko ada dalam Tabel 1 berikut:

Tabel.1. Kriteria pengukuran risiko

Lembar Kerja Allegro	**Kriteria Pengukuran Risiko dan Kepercayaan Pelanggan**
Prioritas	**Dampak area**
I	Kesehatan dan keamanan
II	Kepercayaan pelanggan dan reputasi
III	Keuangan
IV	Produktivitas
V	Denda dan gugatan

3.2. Sumber Daya Data Profil

Dari analisis, di tahap *profiling* sumber laporan dilakukan proses *profiling* sumber laporan berdasarkan aset Puskesmas XYZ. Hasil analisis yang diperoleh penulis disajikan dalam Tabel 2 yaitu:

Tabel 2. Membangun sumber informasi

Allegro Workshet	***Critical Information Asset Profile***	
Critical asset	Apa *asset* informasi penting?	Data *user*
Rationable for selection	Mengapa informasi tersebut menjadi *asset* bagi organisasi	Pengguna harus *login* untuk mengakses informasi yang terdapat pada aplikasi Puskesmas XYZ
Description	Apa deskripsi yang disepakati dari *asset* informasi ini	Berisi *username, password* dan izin akses untuk mengakses aplikasi Puskesmas XYZ
Owner (s)		Bidang pengelolaan puskesmas XYZ
Security recuirements	Persyaratan keamanan apa yang berlaku untuk aset informasi?	
Confidentiality	Hanya personel yang berwenang yang dapat melihat sumber informasi berikut	Pengelola SI Puskesmas XYZ
Integrity	Hanya personel yang berwenang yang dapat melihat sumber informasi berikut	Pengelola SI Puskesmas XYZ
Availability	Asset ini harus tersedia bagi staf untuk melakukan pekerjaan mereka Asset ini harus tersedia selama 24 jam, 7 hari seminggu	Pengelola SI Puskesmas XYZ
Most important security requirement Apa persyaratan keamanan terpenting untuk informasi?		
Kerahasiaan	Integritas	Ketersediaan

3.3. Identifikasi Kontainer dan Aset Informasi

Berdasarkan analisis penulis terhadap fase identifikasi dan sumber daya data, perlu dilakukan identifikasi setiap tempat yang menyimpan dan memproses baik secara internal maupun eksternal. Berdasarkan hasil analisis penulis Tabel 3 dibagi menjadi tiga kategori yaitu teknik, fisik dan manusia, yang dapat dilihat sebagai berikut:

Tabel 3. Lingkungan risiko aset informasi (teknis)

Kategori	Deskripsi	*Owner*
Internal	*Web server* dan *Database server*	Pengelola SI Puskesmas XYZ
	Komputer dan laptop	Pengelola Sarpras Puskesmas XYZ
	Jaringan Internal (LAN)	Pengelola SI Puskesmas XYZ
Eksternal	*Internet Server Provider* (ISP)	Vendor Pihak Ke 3

Pada lingkungan risiko aset informasi mengidentifikasi semua Sistem Informasi Puskesmas XYZ baik dari internal maupun eksternal.

Tabel 4. Lingkungan risiko sumber daya informasi (fisik)

Kategori	Deskripsi	*Owner*
Internal	*Form* Registrasi *User*	Pengelola SI Puskesmas XYZ

Pada lingkungan risiko sumber daya informasi mengidentifikasi yang berkaitan dengan fisik pada Sistem Informasi Puskesmas XYZ hanya kategori internal yang berhubungan dengan form registrasi *user*.

Tabel 5. Lingkungan risiko aset informasi (orang)

Kategori	Deskripsi	*Owner*
Internal	Pelaksana pengelola SI Puskesmas XYZ	Pengelola SI Puskesmas XYZ

Dalam lingkungan aset informasi sistem informasi Puskesmas XYZ mengidentifikasi kategori internal pada pelaksana pengelola Sistem Informasi.

3.4. Identifikasi Area Masalah

Dari analisis, pada tahap mengidentifikasi area masalah perlu dilakukan identifikasi masalah yang diatur sedemikian rupa sehingga dapat merusak aset informasi seluruh Puskesmas dengan mengelompokkan tindakan-tindakan tersebut. Mengidentifikasi *area of concern* dengan memeriksa setiap tempat untuk melihat dan mengidentifikasi *area of concern* yang mungkin dipertahankan, mendokumentasikan setiap bidang minat yang telah ditentukan. *Area of concern* meluas mendapatkan skenario ancaman dan kemudian merekamnya untuk melihat apakah ini memengaruhi persyaratan keamanan. Hasil analisis identifikasi wilayah masalah penulis yaitu pada Tabel 6.

Tabel 6. Identifikasi

No.	*Area of Concern* – Pengguna Data
1	Data pengguna yang terdapat pada *database* Puskesmas telah rusak.
2	Pelaksanaan hak akses untuk meminta informasi layanan yang sedang dalam proses.
3	Penyalahgunaan hak akses ke data pengguna.
4	Pemalsuan data terhadap data pengguna.
5	Kebocoran data permintaan *user.*
6	Pemanfaatan kerentanan dalam akses pihak eksternal dan internal yang tidak diketahui identitasnya terhadap keamanan sistem informasi.
7	Kesalahan saat memasukkan data pengguna ke dalam sistem Puskesmas.
8	Kehilangan data pengguna karena pencadangan gagal.

3.5. Identifikasi Skenario Ancaman

Berdasarkan analisis penulis pada tahap identifikasi skenario ancaman yaitu dengan risiko *database* yang ada. Hasil analisis ditunjukkan pada Tabel 7 sebagai berikut:

Tabel 7. Identifikasi skenario ancaman

Information Asset	Data *User*
Area perhatian	Pemanfaatan kerentanan dalam akses pihak eksternal dan internal yang tidak diketahui identitasnya terhadap keamanan sistem informasi.
1. *Actor*	*User*
2. *Means*	Eksploitasi kerentanan di server, *database*, atau modul oleh pihak eksternal dan internal.
3. *Motives*	Sengaja dan tidak.

Information Asset	Data *User*
	[v] *Disclosure*
	[v] *Modification*
4. *Outcome*	[v] *Destruction*
	[v] *Interuption*
5. *Security Requirement*	Meningkatkan tingkat keamanan *software, hardware* dan jaringan. Keamanan sistem informasi Puskesmas XYZ dipantau secara berkala.
	[v] *High*
6. *Probability*	[v] *Medium*
	[v] *Low*

3.6. Identifikasi Risiko

Berdasarkan analisis penulis, langkah identifikasi risiko adalah menentukan skenario ancaman yang sudah ada sebelumnya pada lembar kerja risiko sumber informasi yang efektif di Puskesmas XYZ, yang ditunjukkan dalam Tabel 8 berikut:

Tabel 8. Identifikasi risiko

No	*Area of Concern*	*Consequences*
1	Pemanfaatan celah dalam mengakses keamanan informasi oleh pihak luar maupun dalam yang tidak diketahui identitasnya.	Informasi yang dapat diubah karena kerentanan keamanannya dapat mengakibatkan distorsi data atau korupsi yang mengganggu kelangsungan operasi sistem informasi Puskesmas.
2	Penyalahgunaan hak akses terhadap data *user*.	Ada ancaman terhadap keamanan data pengguna yang dapat menyebabkan proliferasi aset penting dan gangguan proses bisnis dan Puskesmas serta risiko korupsi data pengguna.
3	Data pengguna yang ada di database Puskesmas telah rusak	Rusaknya data pengguna di databasePuskesmas. membahayakan keutuhan informasi penting di Puskesmas.
4	Kehilangan data *user* karena tidak melakukan *backup* data.	Proses bisnis Puskesmas terganggu dan mungkin mengalami kerugian yang signifikan akibat hilangnya data-data penting dari Puskesmas.
5	Pemalsuan informasi data terhadap data *user*.	Kesalahan informasi pada data pengguna dapat menyebabkan kurangnya kepercayaan terhadap administrasi Puskesmas.
6	Kesalahan dalam menginput data *user* ke dalam sistem Puskesmas.	Kesalahan dalam entri data dapat merugikan pengguna dan mengganggu pengoperasian sistem.
7	Kebocoran data permintaan *user*.	Informasi permintaan pengguna yang bocor dapat menyebabkan penyalahgunaan oleh pihak yang tidak bertanggung jawab, merugikan pengguna dan Puskesmas.

3.7. Analisis Risiko

Berdasarkan analisis faktor, dilakukan kajian terhadap kriteria pengukuran risiko pada tahap analisis risiko, yaitu mengukur dampak terhadap risiko dengan mengukur tingkat atau nilai risiko relatif. [7] Saat menghitung nilai efek area dan nilai risiko relatif untuk setiap informasi, risiko dapat ditentukan dengan mengalikan prioritas efek area. Ada tiga kelas pengaruh dalam metode *octave-allegro*: Rendah=1, Sedang=2, Tinggi=3. Hasil penentuan skor area dampak ditunjukkan pada Tabel 9 sebagai berikut:

Tabel 9. Penentuan *score*

Area dampak	Prioritas	Skor Area dampak		
		Rendah (n=(1))	Sedang (n=(2))	Tinggi (n=(3))
Reputasi dan kepercayaan pelanggan	2	2	4	6
Keuangan	3	3	6	9
Produktifitas	4	4	8	12
Keamanan & kesehatan	1	1	2	3
Denda & gugatan	5	5	10	15

3.8. Pendekatan Mitigasi

Berdasarkan analisis faktor pada langkah akhir ini dengan menggunakan pendekatan mitigasi, semua risiko yang teridentifikasi ditetapkan berdasarkan skor risiko relatif. [8] [9] Menurut penulis, pendekatan mitigasi ini mendukung rekomendasi status rekomendasi untuk setiap sumur risiko. Berdasarkan matriks risiko relatif pada Tabel 10, maka dapat disimpulkan bahwa pendekatan mitigasi untuk setiap masalah terlihat pada Tabel 10.

ISSN : 2685-1814 (*Print*)
ISSN : 2685-7677 (*Online*)

Tabel 10. Matriks relatif risiko

Matriks Relatif Risiko		
Skor Risiko	**POOL**	**Pendekatan Mitigasi**
30 - 45	I	Mengurangi
16 - 29	II	Menunda
0 - 15	III	Menerima

Tabel 11. Mitigasi

No	Area yang Menjadi Perhatian	Matriks *Relative* Resiko	Pool	Pendekatan Mitigasi
1	Pemanfaatan celah dalam mengakses keamanan SI oleh pihak luar maupun dalam yang tidak diketahui identitasnya	37	1	Mengurangi
2	Penyalahgunaan hak akses terhadap data *user*	29	2	Menunda
3	Pemalsuan informasi data terhadap data *user*	40	1	Mengurangi
4	Kehilangan data *user* karena tidak melakukan backup data	43	1	Mengurangi
5	Adanya kerusakan pada data *user* yang terdapat dalam database Puskesmas	44	1	Mengurangi
6	Kesalahan dalam menginput data *user* kedalam sistem puskesmas	15	3	Menerima
7	Kebocoran data permintaan *user*	36	1	Mengurangi
8	Penyebaran hak akses terhadap data permintaan layanan yang sedang dalam proses	26	2	Menunda

Manajemen risiko adalah tindakan pengendalian risiko untuk meminimalkan kejadian risiko berulang. Pada Puskesmas XYZ menggunakan standar NIST SP 800-53 yang merupakan standar mencakup prosedur penilaian keamanan informasi yang komprehensif. [10] Standar tersebut dapat menjadi pedoman untuk mengukur tingkat resiko keamanan yang terjadi sesuai dengan wilayah perhatian. Dengan demikian Puskesmas XYZ memakai standar tersebut. Peraturan dan rekomendasi berikut berdasarkan NIST SP 800-53 tercantum dalam Tabel 12.

Tabel 12. Kontrol dan rekomendasi

No	Wilayah perhatian	Rekomendasi	Deskripsi
1	Pemanfaatan celah dalam mengakses keamanan SI oleh pihak luar maupun yang tidak diketahui identitasnya	*RA-3 Risk Assesment*	Mengidentifikasi dan mendokumentasikan ancaman dan kerentanan dalam sistem baik internal maupun eksternal
2	Penyalahgunaan hak akses terhadap data *user*	*PE-2 Physical Acces Control*	Melakukan pengecekan dan pengawasan terhadap data *user*
3	Pemalsuan informasi data terhadap data *user*	*AC-4 Informaation Flow Enforcement*	Melakukan pengawasan dan peninjauan terkait informasi pada data *user*
4	Kehilangan data *user* karena tidak melakukan backup data	*CP-2 Contingency Plan*	Mengupayakan rencana cadangan sebagai solusi dari ancaman dan kerentanan risiko serta melakukan backup informasi melindungi kerahasiaan, integritas dan ketersediaan cadangan
5	Adanya kerusakan pada data *user* yang terdapat dalam *database* puskesmas	*CP-9 Information System Backup*	
6	Kesalahan dalam menginput data *user* ke dalam sistem Puskesmas	*IR-4 Incident Handling*	Melakukan pemeriksaan ulang validitas input informasi terhadap data *user*
7	Kebocoran data permintaan *user*	*IA-2 Identification Authentication (organizational users)*	Melakukan pemeriksaan ulang validitas input informasi terhadap data *user*
8	Penyebaran hak akses terhadap data permintaan layanan yang sedang dalam proses		Melakukan pengggantian *username* dan *password* pada *user*

4. KESIMPULAN

Studi ini menyediakan matriks risiko terkait kumpulan berdasarkan manajemen risiko yang digunakan yaitu *octave allegro*. Analisis risiko yang diberikan adalah rekomendasi untuk mitigasi atau penanganan karena bersifat komprehensif. Rekomendasi pengelolaan kemudian dibuat untuk meminimalkan potensi dampak. Pengaruh regional pada metode *octave allegro* adalah reputasi dan kepercayaan finansial pelanggan, produktivitas, kesehatan dan keselamatan, denda dan tuntutan hukum. Identifikasi dari risiko menghasilkan cakupan 8 area fokus yang memberikan hasil mitigasi atas risiko tersebut.

Rekomendasi untuk Puskesmas XYZ adalah untuk sering mengecek informsi visual pada platform Puskesmas XYZ dan memahami ancaman dan risikonya serta harus rutin mengecek keamanan sistem informasinya agar tidak bermasalah. Prosedur manajemen risiko keamanan informasi Puskesmas XYZ didasarkan pada hasil analisis risiko dan rekomendasi kebijakan yang ada sesuai dengan metode *octave allegro*. Puskesmas XYZ memiliki identifikasi risiko ganda dan isu risiko tinggi berdasarkan perhitungan matriks risiko relatif, dan memiliki file cadangan yang telah diuji dan diverifikasi, mempunyai pemulihan data pemakai jika terjadi masalah, serta digunakan program perlindungan dari virus.

REFERENSI

[1] D. A. Jakaria, R. T. Dirgahayu, and Hendrik, "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda *Octave allegro*," *Fak. Huk. UII*, pp. 37–42, 2013.

[2] S. T. A. Ramadhani, "Manajemen Risiko Keamanan Informasi dengan Kerangka Kerja *Octave allegro*: Studi Pemerintah Kabupaten Kulonprogo," 2018.

[3] R. a R. a. C. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing *Octave allegro* : Improving the Information Security Risk Assessment Process," *Young*, no. May, pp. 1–113, 2007.

[4] J. Hom, B. Anong, K. B. Rii, L. K. Choi, and K. Zelina, "The *Octave allegro* Method in Risk Management Assessment of Educational Institutions," *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 167–179, 2020.

[5] B. S. G. Naibaho and D. Tjahjadi, "Kajian Manajemen Risiko Sistem Informasi Menggunakan Metode *Octave allegro*," *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 11, no. 1, p. 131, 2022.

[6] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode *Octave allegro*," *J. Teknol. dan Inf.*, vol. 12, no. 2, pp. 106–117, 2022.

[7] A. Wulansari, "Analisis penilaian risiko keamanan untuk aset informasi pada usaha kecil dan menengah bidang finansial B2B : studi kasus ngaturduit.com = Analysis of risk assessment for information asset in small and medium financial B2B : a case study of ngaturduit ". 2013.

[8] H. Ikhsan, N. Jarti, J. T. U. Baja, P. Studi, T. Industri, and O. Allegro, "Analisis Risiko Keamanan Teknologi Informasi," *J. Responsive*, vol. 2, no. 1, pp. 31–41, 2018.

[9] R. R. Saputra, A. Ambarwati, and E. Setiawan, "Manajemen Risiko Teknologi Informasi Menggunakan *Octave allegro* Pada Pt.Hd," *J. Sains, Teknol. dan Ind.*, vol. 17, no. 1, p. 1, 2020.

[10] N. Budarsa, "Analisis Risiko Keamanan Informasi Menggunakan Metode *Octave allegro* dan Analytical Hirarchy Process pada Data Center Pemerintah Kabupaten Buleleng," pp. 13–15, 2022.

[11] J. J. L. Tobing and A. K. Puspa, "Analisis Manajemen Resiko untuk Evaluasi Aset Menggunakan Metode *Octave allegro*," *Expert J. Manaj. Sist. Inf. dan Teknol.*, vol. 5, no. 1, 2015.

[12] M. Rachmaniah and B. Mustafa, "Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode *Octave allegro*," *J. Pustak. Indones.*, vol. 14, no. 1, pp. 1–9, 2016.

[13] Maček, Davor, I.M., Nikola Ivković. Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods. 2011.

[14] Keating, Corland G. Validating the *Octave allegro* Information Systems Risk Assessment Methodology: A Case Study [Dissertation]. Graduate School of Computer and Information Sciences Nova Southeastern University. 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.