ANALISIS RISIKO KEAMANAN INFORMASI E-GOV SISKEUDES MENGGUNAKAN METODE OCTAVE ALLEGRO

Faulinda Ely Nastiti[*1], Prita Haryani[*2]

[1,3]*Fakultas Ilmu Komputer Universitas Duta Bangsa Surakarta*

[1]faulinda.en@gmail.com , [1]faulinda_ely@udb.ac.id

[2]*Jurusan Informatika Fakultas Teknologi Informasi Institut Sains & Teknologi Akprind Yogyakarta*

[2]pritaharyani@akprind.ac.id

Abstrak— Desa mempunyai peran yang strategis dan penting dalam membantu pemerintah daerah dalam proses penyelenggaraan pemerintahan, termasuk pembangunan. Inovasi teknologi menandai momentum transformasi di segala bidang termasuk bidang keuangan di Pemerintah Desa. Digitalisasi keuangan di Pemerintah Desa diwujudkan dalam bentuk sebuah sistem Aplikasi yaitu Sistem Keuangan Desa (SISKEUDES). Dalam pelaksanaannya Pemerintah Desa bertanggungjawab terhadap data dan informasi yang diinputkan ke dalam Aplikasi Siskeudes berbasis *Cash Management System*, karena itu penting bagi Pemerintah Desa agar memahami risiko terhadap aplikasi yang digunakan. Pada penelitian ini akan dilakukan analisis penerapan *Cash Management System* (CMS) pada Aplikasi Sistem Keuangan Desa (SISKEUDES) dengan Metode Octave Allegro. Identifikasi potensi kerawanan informasi dilakukan untuk mengetahui risiko yang dialami pada penerapan *Cash Management System* (CMS) pada Aplikasi Sistem Keuangan Desa (SISKEUDES). Dari penelitian yang dilakukan menghasilkan 7 area of concern dengan pendekatan mitigasi menghasilkan mitigate berjumlah 3, *defer* berjumlah 3, *accept* berjumlah 1. Prioritas risiko dari aspek *technical container* memiliki relative *risk score* 39 dengan strategi pengurangan risiko *mitigate*. Prioritas risiko dari aspek *physical container* memiliki relative risk score 19 dengan strategi pengurangan *risiko defer*. Prioritas risiko dari aspek people container memiliki relative risk score 20 dengan strategi pengurangan risiko *accept*.

Kata kunci— cash management system, sistem keuangan, siskeudeus, octave allegro, manajemen risiko;

I. PENDAHULUAN

Desa mempunyai peran yang strategis dan penting dalam membantu pemerintah daerah dalam proses penyelenggaraan pemerintahan, termasuk pembangunan. Undang-Undang Nomor 6 Tahun 2014 Pasal 1 ayat 1 menegaskan bahwa desa adalah kesatuan masyarakat hukum yang memiliki batas wilayah yang berwenang untuk mengatur dan mengurus urusan pemerintahan, kepentingan masyarakat setempat berdasarkan prakarsa masyarakat, hak asal usul, dan hak tradisional yang diakui dan dihormati dalam sistem pemerintahan NKRI.

Inovasi teknologi menandai momentum transformasi di segala bidang termasuk bidang keuangan di Pemerintah Desa. Sesuai Permendagri Nomor 20 Tahun 2018, Pengelolaan keuangan Desa yang meliputi perencanaan, pelaksanaan, penatausahaan, pelaporan, dan pertanggungjawaban. Karena begitu banyaknya dana transfer yang masuk ke Desa, maka Aplikasi Sistem Keuangan Desa diperlukan untuk memudahkan Pemerintah Desa dalam mengelola keuangan. Digitalisasi keuangan di Pemerintah Desa diwujudkan dalam bentuk sebuah sistem Aplikasi yaitu Sistem Keuangan Desa (SISKEUDES).

Di tahun 2020 seluruh Desa se-Kabupaten Sragen sudah menerapkan Aplikasi Siskeudes secara *on-line*. Karena itu untuk meminimalisir penyalahgunaan anggaran di Desa, diperlukan sebuah sistem *Cash Management System* pada Aplikasi Siskeudes dimana saat ini yang digunakan adalah *Cash Management System* Bank Jateng. Dengan adanya aplikasi tersebut diharapkan Desa lebih transparan, partisipatif, akuntabel, serta dilakukan dengan tertib dan disiplin anggaran agar berjalan baik sesuai visi, misi. Serta dapat melakukan monitoring transaksi keuangan melalui fasilitas internet online setiap saat.

Dalam pelaksanaannya Pemerintah Desa bertanggungjawab terhadap data dan informasi yang diinputkan ke dalam Aplikasi Siskeudes berbasis *Cash Management System* Bank Jateng, karena itu penting bagi Pemerintah Desa agar memahami risiko terhadap Aplikasi yang digunakan. Oleh sebab itu perlu dilakukan identifikasi potensi kerawanan atau kerentanan *(vulnerabilities)* informasi yang ada untuk meneliti risiko yang dialami menggunakan metode Octave Allegro.

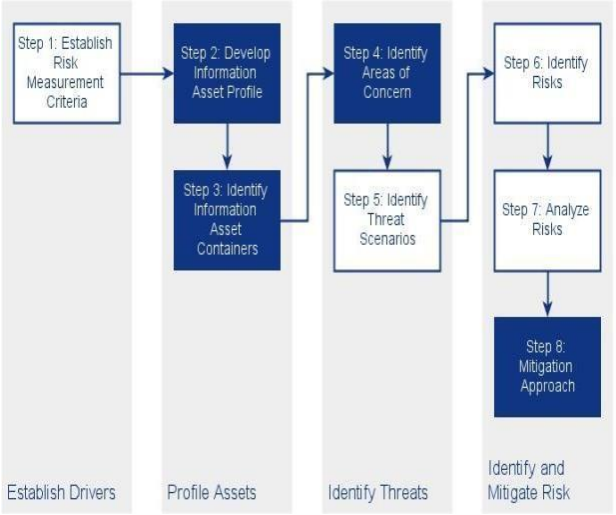
Beberapa penelitian sebelumnya yang relevan dengan penelitian menggunakan metode Octave Allegro untuk menganalisis potensi risiko pada aplikasi sistem informasi adalah penelitian tentang analisis penilaian resiko terhadap perusahaan berbasis finansial planner. Dari hasil analisis resiko yang telah dilakukan, perusahaan harus merumuskan seperangkat peraturan tertulis mengenai kewajiban dan tanggung jawab dalam memelihara informasi perusahaan dan *punishment* bagi yang melanggar, simulasi visual dalam memahami pentingnya aset informasi, potensi ancaman dan risiko, serta waktu efektif untuk evaluasi keamanan informasi adalah secara berkala satu tahun sekali [1]. Penelitiannya lainnya yaitu yang mengevaluasi ancaman dan resiko keamanan informasi melalui parameter *confidentiality*, *integrity*, dan *availability* dari aset-aset informasi kritikal. Pengelolaan aset informasi perlu ditingkatkan karena rentan terjadi ancaman dan dapat berpengaruh terhadap kinerja perusahaan [2]. Dari hasil analisis resiko keamanan informasi dapat dijadikan landasan atas kebijakan dokumen Sistem Manajemen Keamanan Informasi sebagai kerangka acuan yang dapat digunakan untuk meminimalisir resiko keamanan informasi di masa yang akan datang [3]

Fokus utama dari metode OCTAVE Allegro adalah pada aset informasi, dalam konteks yaitu bagaimana mereka digunakan, dimana mereka disimpan, diangkut, diproses dan bagaimana keadaannya jika terkena ancaman, kerentanan, dan gangguan sebagai hasil yang ditimbulkan. Pada penelitian ini akan dilakukan analisis penerapan *Cash Management System* (CMS) pada Aplikasi Sistem Keuangan Desa (SISKEUDES) dengan Metode Octave Allegro. Identifikasi potensi kerawanan informasi dilakukan untuk mengetahui risiko yang dialami pada penerapan *Cash Management System* (CMS) pada Aplikasi Sistem Keuangan Desa (SISKEUDES)

II. METODE PENELITIAN

Pada penelitian ini menggunakan metode *Octave Allegro* untuk untuk mengidentifikasi dan mengevaluasi dari risiko keamanan sebuah sistem informasi. Metode Octave merupakan singkatan dari *The Operationally Critical Threat, Aset, and Vulnerability Evaluation*. Metode Octave melakukan penilaian risiko berdasarkan pada tiga prinsip dasar administrasi keamanan, yaitu*: confidentiality, integrity, availability.* Octave mempunyai dua varian, yaitu octave-s dan octave allegro.

Metode penilaian risiko OCTAVE Allegro dibuat oleh Carnegie Mellon University Software Engineering Institute (SEI) yang memiliki kemampuan untuk memberikan hasil penilaian risiko yang kuat, dengan investasi yang relatif kecil dalam waktu dan sumber daya, bahkan untuk organisasi-organisasi yang tidak memiliki keahlian manajemen risiko yang luas [4]. Salah satu kelebihan OCTAVE Allegro selain cocok untuk digunakan oleh individu yang ingin melakukan penilaian risiko yang *komprehensif* tanpa keterlibatan yang luas dari organisasi, ahli atau sumber daya yang ada juga memiliki kelebihan lainnya yaitu OCTAVE Allegro direkomendasikan untuk peniaian risiko container informasi.



Gambar 1. Langkah – langkah metode OCTAVE Allegro [5]

Setiap tahapan dari delapan tahapan di atas, maka dirinci lagi menjadi beberapa aktivitas penilaian risiko yang akan dilakukan. Untuk memudahkan implementasinya maka OCTAVE Allegro memberikan panduan berupa worksheet 1 sampai 10 seperti tabel 1.

Tabel 1. Tahapan OCTAVE Allegro [5]

Tahap	Aktivitas	Ouput	***Worksheet*/ Acuan**
1	Membangun Kriteria Pengukuran Risiko	Kriteria pengukuran risiko terhadap arahan organisasi, Peringkat area dampak dari yang paling penting hingga yang tidak penting	*Allegro Worksheet* 1-5 dan 6-7
2	Mengembangkan Profil Aset Informasi	Profil aset informasi kritis	*Allegro Worksheet* 8
3	Mengidentifikasi Kontainer dari Aset Informasi	Pemetaan lingkungan risiko aset informasi	*Allegro Worksheet* 9a, 9b, dan 9c
4	Mengidentifikasi *area of conceren* (area yang bermasalah)	Peta lingkungan risiko aset informasi	*Allegro Worksheet* 10

5	Mengidentifikasi Skenario ancaman	Informasi detail dan hasil pengembangan skenario ancaman dari *area of concern*, Daftar risiko aset informasi	Output tahap 4 (*Information Asset Risk Environment Maps*) *Worksheet* 10 *Information Asset Risk Worksheets*
6	Mengidentifikasi Risiko	Konsekuensi dari skenario ancaman **Ancaman (kondisi) +Konsekuensi (dampak) =Risiko [Langkah 4=5] + [langkah 6] = Risiko**	*Information Asset Risk Worksheet*
7	Analisis Risiko	Tabel area dampak Tabel skor risiko	*Risk measurement Criteria, Information Asset Risk Worksheet* 10
8	Memilih Pendekatan Mitigasi	Matriks risiko relatif, Tingkat kerawanan informasi, Mitigasi untuk semuas daftar risiko, Strategi mitigasi untuk setiap risiko yang telah diputuskan untuk dilakukan mitigasi	

III. PEMBAHASAN

Pada bagian ini akan dibahas mengenai langkah-langkah yang dilakukan dalam menganalisis penerapan *Cash Management System* (CMS) pada Aplikasi Sistem Keuangan Desa (SISKEUDES) dengan Metode Octave Allegro.

1) Membangun *Risk Measurement Criteria*

Aktivitas pertama adalah menetapkan *drivers* sebuah organisasi atau instansi terkait dengan mengajukan beberapa pertanyaan untuk memilih *impact area* yang terpenting. Dalam OCTAVE Allegro terdapat 5 *impact area* yang diukur dengan ukuran *low*, *medium* atau *high*. Reputasi dan kepercayaan user, finansial dan produktivitas dipilih sebagai *impact area*.

Tabel 2. *Allegro Worksheet*-1 (*Impact Area* – Reputasi dan Kepercayaan *user*)

Allegro Worksheet 1	***Risk Measurement Criteria – Rreputasi dan Kepercayaan User***		
Impact Area	***Low***	***Medium***	***High***
Reputasi dan kepercayaan customer	Kepercayaan Pemerintah Desa terhadap CMS Siskeudes sedikit sekali atau tidak terpengaruh	Kepercayaan Pemerintah Desa terhadap CMS Siskeudes terpengaruh	Kepercayaan Pemerintah Desa terhadap CMS Bank Jateng sangat terpengaruh
	Dibutuhkan usaha kecil atau tidak ada usaha untuk perbaikan	Dibutuhkan usaha untuk perbaikan relatif lama	Dibutuhkan usaha untuk perbaikan sangat lama.
	Reputasi dan kepercayaan user menurun sebanyak 40%	Reputasi dan kepercayaan user menurun sebanyak 40% hingga 70%	Reputasi dan kepercayaan user menurun dari 70%
Kehilangan user	Dampak kehilangan user tidak ada, karena CMS Siskeudes hanya tool pendamping dan penggunanya merupakan intern Pemerintah Desa. Di sisi lain penggunaan CMS Siskeudes ini terikat dengan peraturan bahwa Pemerintah Desa wajib menggunakannya		

Selanjutnya membuat prioritas *impact area* yang terpenting mendapatkan skor tertinggi dan yang tidak begitu penting mendapatkan skor terendah. Tabel III menunjukan hasil dari penetapan skor *impact area.*

Tabel 3. *Impact Area Prioritization*

Allegro Worksheet 7	***Worksheet Skor Prioritas Impact Area***
Prioritas	***Impact***
1	Reputasi dan Kepercayaan Pengguna
2	Keamanan
3	Produktivitas
4	Hukum dan Peraturan
5	Keuangan atau Biaya operasional
6	Kesehatan dan Keselamatan

2) Mengembangkan Profil Aset Informasi

Aktivitas pertama diawali dengan mengidentifikasi kumpulan aset-aset kritis CMS. Hasil dari indentifikasi dapat dilihat pada tabel IV.

Tabel 4. Daftar aset kritis CMS

NO	Aset-aset	Aset-Aset Kritis
1.	Informasi	*Database* Informasi a. Data Rekening b. Data Transaksi c. Data Admin/operator d. Konten-konten utilitas (info user, info dinas, ubah password, ubah PIN)
2.	Sistem	Aplikasi CMS Bank Jateng dan Aplikasi Siskeudes.
3.	*Hardware*	*Server, Router, Switch/Hub, Acces Point Wireless*, Komputer/Laptop, HP.
4.	*Software*	Sistem Web Based, Php MySQL.
5.	Sumber Daya Manusia	Operator, Checker, Executor

Aktivitas selanjutnya yaitu mendokumentasikan hasil dari *profilling* masing-masing aset infromasi kritis mengacu pada aset-aset informasi kritis pada tabel IV. Berikut contoh dari *profilling* aset informasi seperti pada tabel V dibawah ini.

Tabel 5. *Profilling* Aset Informasi

Aset Kritis	*Aset Informasi*	
Deskripsi	*Database* Informasi a. Data Rekening b. Data Transaksi c. Data Admin/operator d. Konten-konten utilitas (info user, info dinas, ubah password, ubah PIN)	
Pemilik	Operator, Checker, Executor	
Security		
Confidentiality	Layanan infromasi CMS hanya boleh diakses digunakan oleh pihak yang mendapatkan hak akses.	Operator (Sekretaris Desa), Checker (Sekretaris Camat), Executor (Kepala Desa).
Integrity	Layanan informasi CMS harus jelas, benar dan akurat. Dapat diganti dan diubah hanya oleh pihak yang berwenang saja seperti sesuai tingkat wewenangnya.	Operator untuk entry data, Sekretaris Camat sebagai Checker dan Kepala Desa sebagai Executor .
Avaibility	Layanan infromasi CMS harus tersedia untuk seluruh Pemerintah Desa, Pemerintah Kabupaten dan Operator selama 24 jam 7 hari.	Pemadaman akan menjadi masalah. Lebih dari 2×24 jam akan menyebabkan backlog yang signifikan

3) Mengidentifikasi *Containers* dari Aset Informasi Melakukan identifikasi terhadap setiap *container* aset informasi. *Container* tersebut meliputi *technical container (Software, hardware*, sistem, *server*, perangkat jaringan), *physical container* (meliputi item-item dalam bentuk fisik seperti file folder) dan *people container* yang berasal dari internal atau *eksternal* instansi dengan melakukan wawancara pihak terkait. Kemudian dilanjutkan merangkum dan didokumentasikan menggunakan *Information Risk Environtment Map*.

4) Mengidentifikasi *Areas of Concern*

Langkah yang dilakukan adalah mengidentifikasi *areas of concern* di sisi *technical* (TC), *physical* (PC) dan *people* (PC). *Areas of concern* adalah pernyataan deskriptif yang menjabarkan kondisi atau situasi yang sebenarnya yang dapat mempengaruhi aset informasi CMS. Pencatatan *areas of concern* berpedoman pada dokumen *Information Assets Risk Environment Maps*. Tabel IX berikut ini menunjukan daftar *area of concern* yang teridentifikasi.

Tabel 6. *Area of concern*

Area of concern	**Kode**	**Jenis serangan yang terjadi**	***Security Requirments***
Berhentinya layanan CMS dikarenakan *supply* listrik terhenti	TC-1	-	*Avaibility*
Pengeksplotasian celah keamanan CMS oleh pihak luar atau dalam Pemerintah Desa.	TC-2	1. Virus 2. Trojan 3. Worm 4. Spyware 5. DdoS 6. Deface 7. Sistem Crash	*1. Confidentiality* *2. Integrity* *3. Avaibility*
Bocornya hak akses seperti *username* dan *password*.	TC-3	1. SQL Injection 2. Sniffing Jaringan	*1. Confidentiality* *2. Integrity*
Ruangan operator yang mudah diakses mengakibatkan server dapat diakses oleh pihak yang tidak berwenang	TC-4	1. Password Cracking 2. Rootkit	*1. Confidentiality* *2. Integrity* *3. 3) Avaibility*
Penyalahgunaan Hardisk eksternal dan file folder back up data operator oleh pihak yang tidak bertanggung jawab	PC-1	-	*1. Confidentiality* *2. Integrity*

5) Mengidentifikasi *Threat Scenario*

Aktifitas pertama yang dilakukan adalah mengidentifikasi *area of concern* tambahan yang yang sudah ada pada tabel VI dengan menggunakan kuesioner *Appendix C-Threat Scenarios Questionares*. Aktivitas selanjutnya adalah memperluas masing-masing *areas of concern* aspek *technical containers* (TC), *physical containers* (PhC), *people containers* (PC) menjadi *threat scenarios* dengan mengidentifikasi *properties of threat* dari masing-masing *area of concern*.

6) Mengidentifikasi Risiko

Aktivitas yang dilakukan pada langkah ini adalah bagaimana *threat scenario* dapat memberi dampak pada instansi yang dicatat dalam *Information Assets worksheet* bagian ke-7. Aktivitas selanjutnya adalah dengan penentuan *relative score* setiap *impact area*.

7) Menganalisis Risiko

Melakukan analisis risiko pada setiap *areas of concern* serta konsekuensi yang terjadi berdasarkan *relative risk score* dengan mempertimbangkan *risk measurement criteria* yang di ciptakan pada langkah 1.

8) Memilih Pendekatan Mitigasi

Aktivitas pertama yang dilakukan pada langkah ini adalah melakukan pendekatan mitigasi dengan melakukan klasifikasi pada setiap *areas of concern* yang telah diidentifikasi berdasarkan *relative risk score*. Aktivitas selanjutnya adalah menentukan pendekatan mitigasi yang sesuai untuk setiap *areas of concern.* Tabel VII merupakan hasil pemilihan pendekatan mitigasi untuk setiap *area of concern*

Tabel 7. Penentuan mitigasi

Kode	**Area of Concern**	**Relative Risk Score**	**Probabilitas**	**Pool**	**Pendekatan mitigasi**
TC-1	Berhentinya layananCMS yang dikarenakan supply listrik terhenti pada server dan akibat serangan	25	*Low*	Pool 2	Defer
TC-2	Pengeksplotasian celah keamanan CMS oleh pihak luar atau dalam.	39	*High*	Pool 1	Mitigate
TC-3	Bocornya hak akses seperti *username* dan *password*.	29	*Low*	Pool 2	Defer
TC-4	Ruangan operator yang mudah diakses mengakibatkan server dapat diakses oleh pihak yang tidak berwenang.	33	*Medium*	Pool 2	Mitigate
TC-5	Terjadinya bencana alam yang menyebabkan kerusakan pada perangkat-perangkat yang terkait dengan CMS.	31	*Low*	Pool 2	Mitigate
PhC-1	Penyalahgunaan Hardisk eksternal dan file folder back up data operator IT oleh pihak yang tidak bertanggung jawab	19	*High*	Pool 3	Accept
PC-1	Sosial Enginering terhadap operator IT yang mengakibatkan terungkapnya hak server operator IT.	20	*Low*	Pool 3	Defer

Pada *area of concern* TC-2 (Pengeksplotasian celah keamanan CMS oleh pihak luar atau dalam sekolah) mitigasi yang dilakukan adalah *Mitigate* . Hal ini dikarenakan risiko tersebut menempati POOL 1 berdasarkan *relative risk matrix* dengan *relative risk score* 39. *Mitigate* dipilih karena risiko ini mungkin saja dapat terjadi setiap bulan karena banyaknya celah keamanan yang dapat di eksploitasi.

Rekomendasi Mitigasi yang dapat dilakukan antara lain sebagai berikut:

a. Menata ulang konfigurasi desain jaringan yang rawan terhadap keamanan.
b. Mengonfigurasi, mengupgrade dan melakukan *patching* konfigurasi *default* pada perangkat jaringan.
c. Menutup port yang tidak dibutuhkan sebagai upaya mengamankan server, jika perlu dilakukan penggantian port asli.

IV. KESIMPULAN

Berdasarkan hasil analisis yang dilakukan pada Aplikasi *Cash Management System* pada Bank Jateng dalam Aplikasi Siskeudes sudah efektif. Selain itu CMS juga sudah memberikan informasi yang jelas terkait dengan keadaan operasional Pemerintah Desa dan juga dirasa membantu apabila dibandingkan dengan proses secara manual serta memudahkan dalam hal efisiensi waktu dan informasi yang

dihasilkan dinilai lebih mudah dipahami dibandingkan dengan sebelum memakai CMS.

Dengan menggunakan metode OCTAVE Allegro maka dapat disimpulkan bahwa terdapat 6 area dampak yaitu reputasi dan kepercayaan pengguna, keamanan, produktivitas, hukum dan peraturan, keuangan atau biaya operasional dan kesehatan dan keselamatan. Dengan menggunakan metode OCTAVE Allegro dapat diidentifikasi impact areas penting yang menjadi indikator dalam penilaian dan mitigasi risiko yang nantinya akan digunakan, yaitu *Confidentiality*, *Integrity*, *Availability.*

Dari penelitian yang dilakukan menghasilkan 7 area of concern dengan pendekatan mitigasi menghasilkan mitigate berjumlah 3, *defer* berjumlah 3, *accept* berjumlah 1. Prioritas risiko dari aspek *technical container* memiliki relative *risk score* 39 dengan strategi pengurangan risiko *mitigate*. Prioritas risiko dari aspek *physical container* memiliki relative risk score 19 dengan strategi pengurangan *risiko defer*. Prioritas risiko dari aspek people container memiliki relative risk score 20 dengan strategi pengurangan risiko *accept*.

REFERENSI

[1] J. Sanjaya, "Analisis Risk Assessment Terhadap Perusahaan It Di Bidang Finansial Menggunakan Octave Allegro Framework," *Jurnal Teknologi Informasi Dan Komunikasi,* Vol. 10, No. 1, Pp. 57-67, 2020.

[2] R. R. Saputra, E. Setiawan And A. Ambarwati, "Manajemen Risiko Teknologi Informasi Menggunakan Metode OCTAVE Allegro Pada PT. Hakiki Donarta Surabaya," *Urnal Sains, Teknologi Dan Industri,* Vol. 17, No. 01, Pp. 1-10, 2019.

[3] F. I. And N. Mutiah, "Analisis Dan Perancangan Sistem Manajemen Keamanan Informasi Pada Kantor Imigrasi Kelas 1 Tpi Pontianak Menggunakan Metode Octave Allegro Dan Iso/Iec 27001:2013," *Jurnal Komputer Dan Aplikasi,* Vol. 8, No. 1, Pp. 152-162, 2020.

[4] C. G. Keating, Validating The OCTAVE Allegro Information Systems Risk Assessment Methodology : A Case Study., Florida: Computer And Information Sciences. Nova Southeastern University, 2014.

[5] H. Ikhsan And N. Jarti, "Analisis Risiko Keamanan Teknologi Informasi Menggunakan Octave Allegro," *Jurnal Responsive Teknik Informatika,* Vol. 2, No. 1, Pp. 31-41, 2018.