# Penilaian Risiko Aset Informasi dengan Metode OCTAVE Allegro: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya

**Aulia Zulfia[1], Endang Lestari Ruskan[2], Pacu Putra[3]**
Fakultas Ilmu Komputer Universitas Sriwijaya
e-mail: [1]auliazul30@gmail.com, [2]endanglestari@unsri.ac.id, [3]pacu89@gmail.com

Diterima: 24 September 2020; Disetujui: 12 April 2021

***Abstrak***

*Informasi yang merupakan aset berharga bagi organisasi sangat penting dikelola risikonya agar dapat mempertahankan kelangsungan bisnis. ICT Fakultas Ilmu Komputer Universitas Sriwijaya (Fasilkom Unsri) memiliki aset informasi yang harus dilindungi terhadap ancaman baik dari pihak luar maupun dalam. Namun, sayangnya ICT Fasilkom Unsri belum pernah melakukan penilaian risiko dan belum memiliki prosedur secara formal/tertulis mengenai mitigasi risiko. Oleh karena itu, ICT Fasilkom Unsri belum mengetahui tindakan apa yang tepat untuk mengurangi risiko yang akan terjadi. Metode OCTAVE Allegro digunakan untuk membantu organisasi mengidentifikasi, menganalisis, dan mengambil tindakan mitigasi. Berdasarkan hasil penelitian, 5 dari 7 aset informasi yang dikelola oleh ICT Fasilkom Unsri dianggap sebagai aset yang kritikal. Setelah diidentifikasi dan dianalisis, ditemukan 73 risiko keamanan informasi Tindakan yang dapat diambil antara lain, 61 risiko dimitigasi/ditunda, 3 risiko ditunda/diterima, dan 3 risiko diterima. Dengan mengetahui penilaian risiko dari tiap-tiap aset informasi, ICT Fasilkom Unsri dapat membuat keputusan dalam pengurangan risiko secara tepat sesuai dengan kemungkinan-kemungkinan risiko yang akan terjadi.*

***Kata kunci:*** *Penilaian Risiko, Manajemen Risiko, Aset Informasi, OCTAVE Allegro*

***Abstract***

*Information is a valuable asset for an organization and it is very important to manage the risk of it in order to maintain business continuity. ICT Faculty of Computer Science, Sriwijaya University (Fasilkom Unsri) has information assets that must be protected against threats from both outside and inside. Unfortunately, ICT Fasilkom Unsri has never conducted a risk assessment and does not have a formal or written procedure regarding risk mitigation. Therefore, ICT Fasilkom Unsri does not know what actions are appropriate to reduce the risks that will occur. The OCTAVE Allegro method is used to help organizations to identify, analyze and mitigate. Based on the research results, 5 of the 7 information assets managed by ICT Fasilkom Unsri are considered critical assets. Once identified and analyzed, 73 information security risks were found. Actions that can be taken included, 61 risks to be mitigated or postponed, 3 risks to be postponed or accepted, and 3 risks to be accepted. The advantage of knowing the risk assessment of each information asset for ICT Fasilkom Unsri is, they can make decision in reducing risk appropriately according to the possible risks that will occur.*

***Keywords****: Risk Assessment, Risk Management, Information Asset, OCTAVE Allegro*

## 1. PENDAHULUAN

Saat ini teknologi informasi bukan hanya digunakan untuk mendukung proses bisnis, namun juga digunakan untuk mendukung strategi bisnis organisasi dan meningkatkan kualitas layanan [1]. Di dalam organisasi, informasi merupakan salah satu aset takberwujud (*intangiable asset)* yang harus dilindungi untuk menjamin kelangsungan organisasi [2]. Dalam penggunaannya, dimungkinkan terjadinya suatu peristiwa yang tidak diinginkan sehingga penting bagi organisasi untuk mengelola risiko yang dapat membahayakan aset informasi [3].

Manajemen risiko diperlukan oleh organisasi karena dapat menentukan keamanan aset informasi dengan cara yang paling efektif dengan biaya yang efisien [4]. Di dalam manajemen risiko terdapat penilaian risiko atau dikenal dengan analisis risiko untuk menilai seberapa sering risiko terjadi dan seberapa besar dampak dari risiko. Penilaian risiko ini melibatkan identifikasi dan penilaian risiko terhadap kerahasiaan, integritas, dan ketersediaan sistem informasi dan sumber daya [5]. Metode OCTAVE Allegro merupakan salah satu metode dalam penilaian risiko.

Metode OCTAVE (*Operationally, Critical Threat, Asset, and Vulnerability Evaluation*) melakukan penilaian risiko berdasarkan tiga prinsip dasar administrasi keamanan, yaitu: kerahasiaan, integritas, dan ketersediaan [6]. Berbeda dengan metode OCTAVE terdahulu, yaitu OCTAVE dan OCTAVE-S, fokus utamanya adalah aset informasi yang dalam konteks bagaimana aset tersebut digunakan, diangkut, diproses dan bagaimana aset terkena ancaman, kerentanan, dan gangguan sebagai hasilnya [7].

Penelitian ini bertujuan untuk melakukan penilaian risiko pada aset informasi pada ICT Fakultas Ilmu Komputer (Fasilkom) Universitas Sriwijaya (Unsri). Berdasarkan hasil wawancara dengan Manajer Penelitian dan Pengembangan, ICT Fasilkom Unsri belum pernah melakukan penilaian risiko dan belum memiliki aturan/kebijakan secara formal/tertulis mengenai mitigasi risiko sehingga ICT Fasilkom Unsri belum mengetahui tindakan apa yang tepat untuk mengurangi risiko yang terjadi. Untuk mendapatkan hasil penilaian risiko yang cepat dengan minimnya jumlah karyawan, metode OCTAVE Allegro dipilih sebagai metode penilaian risiko [7].

## 2. METODE PENELITIAN

Instrumen penelitian pada penelitian ini menggunakan wawancara semi terstruktur. Sebanyak 10 pertanyaan utama dirancang berdasarkan laporan teknis yang dikeluarkan oleh Software Engineering Institute. Pertanyaan-pertanyaan utama selanjutnya dikembangkan selama wawancara berlangsung untuk mendapatkan informasi lebih mendalam mengenai kriteria pengukuran risiko, aset-aset informasi, dan orang-orang yang terlibat dalam aset tersebut. Hasil dari wawancara kemudian dibuat transkrip dan di-*coding* untuk mendapatkan intisari wawancara.

Metode OCTAVE Allego digunakan sebagai metode analisis data pada penelitian ini. Metode ini merupakan laporan teknis yang diperkenalkan oleh Software Engineering Institute dengan tujuan untuk menghasilkan hasil yang lebih cepat tanpa memerlukan keahlian yang mendalam mengenai penilaian risiko. OCTAVE Allegro berbeda dengan metode OCTAVE lainnya karena fokus dari metode ini adalah aset informasi yang digunakan oleh organisasi, mulai dari bagaimana aset tersebut digunakan hingga bagaimana ancaman maupun kerentanan dapat mengancam aset tersebut [6,7].

Metode OCTAVE Allegro telah banyak diimplementasi di Indonesia, seperti pada perusahaan air kemasan, bank, perpustakaan, dan perguruan tinggi[1,7,8,9,10,11,12] Permasalahan utama yang terjadi pada penelitian-penelitian ini disebabkan karena belum pernah dilakukan penilaian risiko[1,12] tidak adanya kebijakan tertulis yang berhubungan dengan keamanan informasi[1,12], sulitnya menentukan seberapa penting suatu aset informasi[1], dan pernah terjadinya kehilangan data [11]. Beberapa penelitian juga menggunakan metode ini untuk mempertahankan kelangsungan bisnis[10] maupun untuk keunggulan bersaing [7,11].

Terdapat 8 langkah dalam dalam metode OCTAVE Allegro. Gambar 1. Menunjukkan langkah-langkah dalam metode ini.


Gambar 1. Langkah-Langkah Metode OCTAVE Allegro. Sumber [12]

Metode OCTAVE Allegro terdiri dari 8 langkah yang dikelompokkan menjadi empat fase [6]. Fase pertama adalah menentukan penggerak. Dalam fase ini terdapat satu langkah, yaitu menentukan kriteria pengukuran risiko. Penulis membuat kriteria pengukuran risiko berdasarkan hasil wawancara dengan tujuan sebagai acuan dalam penilaian risiko. Setelah mengetahui kriteria pengukuran risiko, lalu prioritas area dampak ditentukan. Kategori yang berdampak besar diberi nilai tertinggi dan yang tidak terlalu berdampak diberi nilai rendah.

Fase kedua adalah membuat profil aset yang terdiri dari dua langkah, yaitu mengembangkan profil aset informasi dan identifikasi kontainer aset informasi. Pada langkah mengebangkan profil aset informasi, semua aset informasi diidentifikasi dan selanjutnya aset yang dianggap krusial yang akan dikembangkan secara spesifik. Setelah itu, kontainer aset informasi juga diidentifikasi. Kontainer aset informasi dapat berupa teknologi (seperti, perangkat lunak, perangkat keras, dan aplikasi) maupun non teknologi (seperti, dokumen, lembaran kertas penting, dan karyawan).

Lalu, di fase selanjutnya adalah mengidentifikasi ancaman. Terdapat dua langkah dalam fase ini, yaitu identifikasi area yang menjadi perhatian dan identifikasi skenario ancaman. Identifikasi area yang menjadi perhatian bertujuan untuk mengambil semua kemungkinan ancaman dan kerentanan yang mungkin akan terjadi. Pada langkah ini semua kemungkinan yang akan terjadi pada tiap-tiap kontainer aset didokumentasikan. Setelah itu, dokumentasi ini diperluas ke tahap selanjutnya, yaitu identifikasi skenario ancaman. Skenario ancaman berisi pendokumentasian lengkap mulai dari pelaku, tujuan, motif, hasil dari ancaman, kebutuhan keamanan, dan tingkat kemungkinan ancaman terjadi.

Fase terakhir dalam metode ini adalah identifikasi dan mitigasi risiko. Fase ini terdiri dari tiga langkah, yaitu identifikasi risiko, analisis risiko, dan pemilihan pendekatan mitigasi. Pada langkah identifikasi risiko, konsekuensi-konsekuensi yang mungkin terjadi ditambahkan kedalam dokumentasi skenario ancaman. Lalu, konsekuensi tersebut kemudian dianalisis. Tujuannya adalah untuk menentukan tindakan yang dapat dilakukan organisasi terhadap risiko yang akan dihadapi. Hasil analisis kemudian diukur tingkat keparahannya dengan menggunakan perhitungan nilai skor relatif. Besar kecilnya skor relatif dapat menentukan bagaimana organisasi akan melakukan pengurangan risiko.

## 3. HASIL DAN PEMBAHASAN

Langkah pertama yang dilakukan sebelum melakukan penilaian risiko adalah menetapkan kriteria pengukuran risiko. Pada langkah ini terdapat dua aktivitas yang harus

dilakukan, yaitu membuat kriteria pengukuran risiko dan mempertimbangkan dan membuat prioritas dari area dampak. Terdapat lima area yang harus ada dalam membangun kriteria pengukuran risiko: reputasi dan kepercayaan konsumen, keuangan, keselamatan dan kesehatan, denda dan sanksi hukum, dan produktivitas. Dalam satu area dampak, terdapat tiga pembagian skala yaitu rendah, sedang, dan tinggi. Setelah menentukan kriteria pengukuran risiko, yang dilakukan selanjutnya adalah membuat prioritas area dampak. Semakin besar nilai prioritas, semakin penting area dampak bagi organisasi.

Berdasarkan hasil wawancara, prioritas area dampak dapat dilihat pada tabel 1. Tabel 1 menunjukkan bahwa Reputasi dan Kepercayaan Konsumen menjadi prioritas utama bagi ICT Fasilkom Unsri. ICT Fasilkom Unsri merupakan penyedia layanan teknologi informasi untuk civitas akademik, sehingga bila terjadi ancaman maka sangat berdampak pada reputasi dan kepercayaan mahasiswa, dosen, maupun civitas lainnya yang menggunakan layanan.

Tabel 1. Prioritas Area dampak

| Prioritas | Area Dampak |
|---|---|
| 5 | Reputasi dan Kepercayaan Konsumen |
| 4 | Keuangan |
| 3 | Produktivitas |
| 2 | Keselamatan dan Kesehatan |
| 1 | Denda dan Sanksi Hukum |

Tahap selanjutnya adalah mengembangkan profil aset dan mengidentifikasi kontainer aset informasi. Aset-aset informasi yang dimiliki ICT Fasilkom Unsri dipilih dan diurutkan berdasarkan tingkah pengaruhnya terhadap kelangsungan belajar mengajar. Setelah diurutkan, terdapat 5 aset informasi yang dianggap sebagai aset yang sangat penting, yaitu: data mahasiswa, data dosen, data pegawai, data alumni, dan data pelacakan alumni. Informasi-informasi yang terkait dengan aset yang kritikal ini dicatat pada tabel 2.

Tabel 2. Identifikasi Kontainer Aset Informasi — Data Mahasiswa

| | | |
|---|---|---|
| *Critical Asset* | Data Mahasiswa | |
| *Rationale for Selection* | Peran mahasiswa sangat penting di setiap proses bisnis Fakultas sehingga bila data mahasiswa rusak/hilang akan berdampak pada kelangsungan aktivitas di Fakultas Ilamu Komputer. | |
| *Description* | NIM, nama mahasiswa, program studi, dan data yang berkaitan dengan akademik mahasiswa. | |
| *Owner(s)* | Syamsuryadi, M. Kom., Ph.D. | |
| *Security Requirement* | *Confidentiality* | Informasi-informasi yang berkaitan dengan data mahasiswa bersifat privasi dan hanya pengguna yang memiliki hak akses (seperti mahasiswa, admin jurusan) yang diperbolehkan untuk mengakses informasi tersebut. |
| | *Integrity* | Hanya mahasiswa itu sendiri yang boleh mengubah/memodifikasi data-data yang terdapat dalam data mahasiswa. |
| | *Availability* | Informasi ini harus tersedia untuk mahasiswa 24 jam/hari |
| *Most Important Security Requirement* | *Integrity* | |

Setelah melakukan pengembangan profil aset, tahap selanjutnya adalah memetakan kontainer aset informasi. Identifikasi ini mencakup aset informasi berupa teknologi (seperti, aplikasi, perangkat lunak, dan perangkat keras), non teknologi (seperti, berkas dokumen, atau formulir), dan manusia. Tabel 3. merupakan hasil pemetaan kontainer aset informasi pada data mahasiswa.

Tabel 3. Pemetaan Kontainer Aset Informasi — Data Mahasiswa

| Kontainer | Lokasi | Deskripsi Kontainer | Pemilik Informasi |
|---|---|---|---|
| Teknikal | Internal | SAFANA: Data mahasiswa diakses pada aplikasi ini untuk keperluan perubahan kata sandi atau pembuatan akun SAFANA untuk pertama kali. | Unit ICT Fasilkom Unsri |
| | | Basis data : Data mahasiswa disimpan di basis data Fakultas untuk aplikasi web. | Unit ICT Fasilkom Unsri |
| | Eksternal | SIMAK (Sistem Informasi Akademik): Data mahasiswa diakses dan diproses di SIMAK untuk perubahan informasi data diri. | Mahasiswa |
| Fisikal | Internal | Surat permintaan data ke ICT Unsri: Staf Unit ICT Fasilkom Unsri meminta data mahasiswa dengan menggunakan surat permintaan data ke ICT Unsri | Unit ICT Fasilkom Unsri |
| | Eksternal | Berkas-berkas mahasiswa saat penerimaan mahasiswa | BAAK (Biro Administrasi Akademis Kemahasiswaan) |
| Manusia | Internal | Tri Wanda Septian, S. Kom | Unit ICT Fasilkom Unsri |
| | | Wisnu Adi Putra, S. Kom | Unit ICT Fasilkom Unsri |
| | Eksternal | Mahasiswa | Mahasiswa |

Aktivitas selanjutnya adalah mengidentifikasi ancaman, mengidentifikasi risiko dan melakukan pendekatan mitigasi. Identifikasi ancaman dilakukan dengan mengumpulkan semua kondisi atau situasi yang akan terjadi bila aset informasi terancam. Kemudian situasi tersebut diperluas menjadi sebuah skenario ancaman. Sedangkan pada identifikasi risiko, semua konsekuensi dari hasil ancaman yang terjadi dicatat dan dilakukan penilaian risiko untuk menentukan tindakan yang harus dilakukan. Dari 5 aset yang kritikal, ditemukan total 73 ancaman dan keretanan keamanan informasi. Hasil identifikasi ancaman pada salah satu aset informasi dapat dilihat pada tabel 4.

Tabel 4. Identifikasi Ancaman — Data Mahasiswa

| *Area of Concern* | *Threat Properties* | |
|---|---|---|
| *Bug/error* yang terdapat pada *website* SAFANA yang muncul ketika staf | Aktor | Staf Unit ICT Fasilkom Unsri |
| | Tujuan | Akses dalam memodifikasi aplikasi SAFANA |

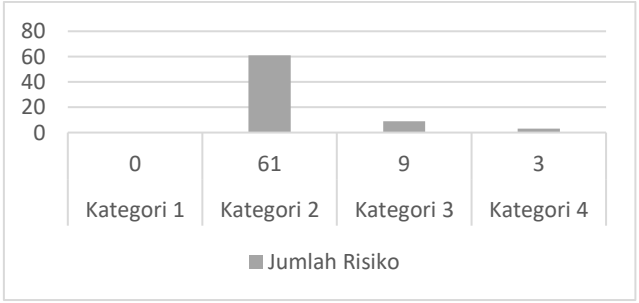
| | | |
|---|---|---|
| melakukan pemeliharaan sistem. | Motif | Human Error |
| | Hasil | Pengungkapan, modifikasi, dan interupsi. |
| | Kebutuhan Keamanan | Dilakukannya *testing* aplikasi sebelum melakukan *deployment* |
| | Kemungkinan | Tinggi |
| *Consequences* | | |
| 1. Dapat mengurangi produktivitas staf sehingga staf hanya fokus pada memperbaiki *bug/error* pada aplikasi SAFANA. Selain itu mahasiswa sulit<br>2. melakukan akses ke SAFANA hingga akhirnya mahasiswa tidak menggunakan aplikasi SAFANA. | | |
| *Severity* | | |
| *Impact Area* | *Value* | *Score* |
| Reputasi & Kepercayaan Pelanggan | Sedang | 10 |
| Finansial | Sedang | 8 |
| Produktivitas | Sedang | 6 |
| Keselamatan & Kesehatan | Rendah | 2 |
| Denda & Sanksi Hukum | Rendah | 1 |
| *Relative Risk Score* | | 27 |

Setelah mengetahui skor risiko, tahap selanjurnya adalah memutuskan tindakan apa yang harus dilakukan. Dalam pendekatan mitigasi, organisasi dapat memilih 3 pilihan, yaitu menerima, mengurangi, atau menunda risiko. Keputusan untuk mengambil sebuah tindakan disesuaikan dengan matriks risiko relatif yang sebelumnya telah dibuat. Matriks risiko relatif ini berisi pengkategorian risiko dan skor pada tiap kategori tersebut. Pengelompokan pendekatan mitigasi berdasarkan skor risiko dapat dilihat pada tabel 5.

Tabel 5. Matrik Risiko Relatif dengan Probabilitas Ancaman

| Probabilitas | Skor Risiko Relatif | | |
|---|---|---|---|
| | 30-45 | 16-29 | 0-15 |
| Tinggi | (Kategori 1) Mitigasi | (Kategori 2) Mitigasi/Menunda | (Kategori 2) Mitigasi/Menunda |
| Sedang | (Kategori 2) Mitigasi/Menunda | (Kategori 2) Mitigasi/Menunda | (Kategori 3) Menunda/Menerima |
| Rendah | (Kategori 3) Menunda/Menerima | (Kategori 3) Menunda/Menerima | (Kategori 4) Menerima |

Berpedoman dengan matrik risiko relatif, pendekatan mitigasi yang dilakukan ICT Fasilkom Unsri dapat dilihat pada gambar 2.




Gambar 2. Pendekatan Mitigasi ICT Fasilkom Unsri Berdasarkan Matriks Risiko Relatif

Berdasarkan gambar 2, kategori 2, yaitu mitigasi/menunda risiko menjadi pendekatan yang paling banyak dilakukan, disusul dengan mitigasi/menerima, dan menerima risiko. Area kerawanan, kontainer, dan kontrol yang harus dilakukan perlu didefinisikan seperti tabel 6.

Tabel 6. Pendekatan Mitigasi — Data Mahasiswa

| Aset Informasi: Data Mahasiswa | |
|---|---|
| Area kerawanan | Aksi |
| Penyebaran data mahasiswa pada pihak-pihak yang memiliki hak akses | Kategori 2-Mitigasi/Menunda |
| Kontainer | Kontrol |
| Staf ICT Fasilkom Unsri | Mengedukasi staf melalui program kesadaran keamanan informasi. |
| Basis data | Mengenkripsi kata sandi mahasiswa, melakukan pembatasan akses, dan membuat batasan durasi sesi *login* |

Tabel 6 menunjukkan kontrol yang harus dilakukan apabila penyebaran data mahasiswa benar-benar dilakukan oleh pihak yang memiliki hak akses. Kontrol pertama dilakukan dari Staf ICT Fasilkom Unsri, yaitu dengan mengedukasi staf melalui program kesadaran keamanan informasi. Lalu, untuk teknikalnya dengan melakukan enkripsi kata sandi, melakukan pembatasan akses data mahasiswa, dan membuat batasan durasi sesi *login*.

## 6. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, didapatkan kesimpulan bahwa terdapat 73 risiko keamanan informasi dari 5 aset informasi yang dianggap kritikal. Dari 73 risiko ini dilakukan penilaian risiko dan didapatkan sebanyak 61 risiko berada pada kategori 2, yaitu mitigasi atau ditunda. Lalu, 9 risiko pada kategori 3, yaitu ditunda atau diterima. Sisanya sebanyak 3 risiko berada pada kategori 4, yaitu diterima. Risiko yang berada pada kategori 4 memiliki risiko yang kecil dibanding usaha untuk mencegahnya. Oleh karena itu, ICT Fasilkom Unsri dapat menerima risiko/membiarkan risiko itu terjadi. Untuk kategori 2 dan 3, ICT Fasilkom Unsri dapat memilih untuk melakukan mitigasi, menunda, atau menerima risiko. Dengan mengetahui penilaian risiko dari tiap-tiap aset informasi, ICT Fasilkom Unsri dapat membuat keputusan dalam pengurangan risiko secara tepat sesuai dengan kemungkinan-kemungkinan risiko yang akan terjadi.

## 5. SARAN

Untuk saran penelitian selanjutnya, ada beberapa hal yang dapat diteliti untuk mendapatkan hasil yang maksimal. Pertama, untuk mendapatkan hasil yang lebih akurat, pengambilan data dapat dilakukan dengan cara *focus group discussion* (FGD) bersama pemangku kepentingan seperti, Dekan dan Ketua Jurusan agar pendekatan mitigasi yang didapat bukan hanya secara teknikal, namun juga secara strategik. Kedua, sebaiknya metode ini dikembangkan lagi dengan mengkombinasikannya dengan metode lain. Terakhir, perlu adanya pengembangan pada teori ini. Di Indonesia, teori ini banyak digunakan pada perguruan tinggi. Untuk penelitian selanjutnya, dapat mengaplikasikannya pada ruang lingkup lain seperti pada UMKM, Perusahaan Asuransi, atau di Pemerintahan.

## DAFTAR PUSTAKA

[1] J. S. Suroso, M. A. Fakhrozi, J. S. Suroso, and M. A. Fakhrozi, "Assessment Of Information System Risk Management with Octave Assessment Of Information Risk Management with Octave Allegro At System Education," *Procedia Comput. Sci.*, vol. 135, pp. 202–213, 2018.

[2] M. Moyo, "Information Security Risk Management in Small-Scale Organisations : A Case Study of Secondary Schools' Computerised Information Systems," University of South Africa, 2014.

[3] B. M. Dioubate, N. N. A. Molok, S. Talib, and A. O. M. Tap, "Risk assessment model for organizational information security," *ARPN J. Eng. Appl. Sci.*, vol. 10, no. 23, pp. 17607–17613, 2015.

[4] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A Situation Awareness Model for Information Security Risk Management," *Comput. Secur.*, vol. 44, pp. 1–15, Jul. 2014.

[5] M. Talabis and J. Martin, *Information Security Risk Assessment Toolkit*. Elsevier, 2013.

[6] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," May 2007.

[7] S. I. Hasibuan, T. F. Kusumasari, and R. Fauzi, "Analisis Risiko Keamanan Informasi dengan Metode Octave Allegro pada PT. Tirta Investama," *e-Proceeding Eng.*, vol. 6, no. 2, pp. 7899–7907, 2019.

[8] W. Sardjono and M. I. Cholik, "Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank," *Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018*, no. September, pp. 38–42, 2018.

[9] D. A. Jakaria and J. T. Informatika, "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro," pp. 37–42, 2013.

[10] Rosini, M. Rachmaniah, and B. Mustafa, "Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allegro," *J. Pustak. Indones.*, vol. 14, no. 1, 2016.

[11] N. L. Kuntari, Y. H. Chrisnanto, and A. I. Hadiana, "Manajemen Risiko Sistem Informasi di Universitas Jenderal Achmad Yani Menggunakan Metoda OCTAVE Allegro," *Semnati*, 2018.

[12] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Pittsburgh, Pennsylvania, 2007.