

## MANAJEMEN RISIKO SISTEM INFORMASI STUDENT SERVICE CENTER MENGUNAKAN METODE OCTAVE ALLEGRO

Ito Setiawan<sup>1</sup>, Riyanto<sup>2</sup>, Ika Romadoni Yunita<sup>3</sup>, Jeffri Prayitno Bangkit Saputra<sup>4</sup>

<sup>1,3,4</sup>Sistem Informasi, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto

<sup>2</sup>Informatika, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto

Email : itosetiawan@amikompurwokerto.ac.id

### ABSTRAK

Universitas Amikom Purwokerto memberikan pelayanan kepada mahasiswa dalam bentuk sistem student service center yang digunakan untuk pengelolaan akademik mahasiswa. Dalam sistem tersebut berisi tentang menu umum, akademik, events, perpustakaan, aktivitas mahasiswa, proses pembelajaran, keuangan dan Lainnya. permasalahan yang sering terjadi pada student service center adalah seringkali terjadi server error pada saat melakukan pengisian KRS online yang mengakibatkan banyaknya mahasiswa yang mendapatkan kelas acak sehingga jadwalnya bertabrakan. Penelitian ini memiliki tujuan untuk menganalisis ancaman, melakukan penilaian dan evaluasi risiko yang terjadi terhadap aset kampus. OCTAVE Allegro merupakan metode yang digunakan untuk menganalisis permasalahan yang ada. Hasil penelitian yaitu terdapat 3 area of concern. Terdapat 4 Impact Area Prioritization dengan urutan prioritas reputasi, produktivitas, keuangan dan keamanan. Pada area of concern eksploitasi celah keamanan sistem terdapat 5 mitigasi. Pada kapasitas ruang penyimpanan terdapat 3 mitigasi dan bagian internet yang tidak stabil terdapat 4 mitigasi. Dari hasil analisis risiko terdapat nilai paling tinggi yaitu 28 adalah area of concern internet yang tidak stabil pada sistem yang digunakan.

Kata Kunci: *Manajemen Risiko, Student Service Center, OCTAVE Allegro*

### ABSTRACT

Amikom Purwokerto University provides services to students in the form of a student service center system that is used for student academic management. The system contains general, academic, events, library, student activities, learning processes, financial and other menus. The problem that often occurs in student service centers is the frequent occurrence of server errors when filling in online KRS which results in many students getting random classes so their schedules collide. This study has the aim of analyzing threats, conducting assessments and evaluating risks that occur to campus assets. OCTAVE Allegro is a method used to analyze existing problems. The results of the study are that there are 3 areas of concern. There are 4 Impact Areas Prioritization in priority order of reputation, productivity, finance and security. In the area of concern for exploiting system security holes, there are 5 mitigations. In terms of storage space capacity, there are 3 mitigations and unstable internet parts, there are 4 mitigations. From the results of the risk analysis, the highest value is 28, which is an unstable internet area of concern in the system used

Keywords: *Risk Management, Student Service Center, OCTAVE Allegro*

## I. PENDAHULUAN

Semakin bertambahnya ketergantungan penggunaan teknologi informasi pada organisasi maka semakin tinggi juga risiko dan ancaman yang mungkin muncul saat teknologi informasi digunakan (Atmojo & Manuputty, 2020). Risiko merupakan kondisi dimana aktivitas yang dilakukan berdampak bagi organisasi yang tidak sesuai dengan gambaran yang diinginkan (Evinia & Sitokdana, 2023) (Fu & Chen, 2021). Penggunaan teknologi informasi pada organisasi memiliki risiko masing-masing seperti kerusakan sistem, human error, kegagalan kelistrikan, internet bermasalah dan banyak lainnya (Ash Siddiqi, Darwiyanto, & Priyadi, 2023) (Setiawan, Sekarini, Waluyo, & Afiana, 2021). Dalam mengurangi risiko yang mungkin terjadi pada penggunaan teknologi maka perlu adanya tata kelola risiko yang baik (Ichsan, Falach, Abdurrahman, Santoso, & Si, 2021), tata Kelola yang baik untuk mengurangi atau mengatasi risiko yang akan terjadi dapat dilakukan dengan manajemen risiko (Diansyah, 2019) (Asrori, Murtiasri, Raharjanti, & Evayanti, 2020). Manajemen risiko merupakan tahapan yang didalamnya terdapat aktivitas seperti mengidentifikasi risiko, mengontrol risiko, dan melakukan mitigasi risiko (Sari, Sakethi, Prabowo, Komputer, & Lampung, 2019) (Syihabuddin, Suryanto, & Salman, 2019). Manajemen risiko yang baik akan mempengaruhi penggunaan teknologi informasi dan manajemen layanan TI (Prabowo, ., A Setiawan, Muslim, & Utama, 2017). Permasalahan penggunaan sistem informasi juga dialami oleh Universitas Amikom Purwokerto.

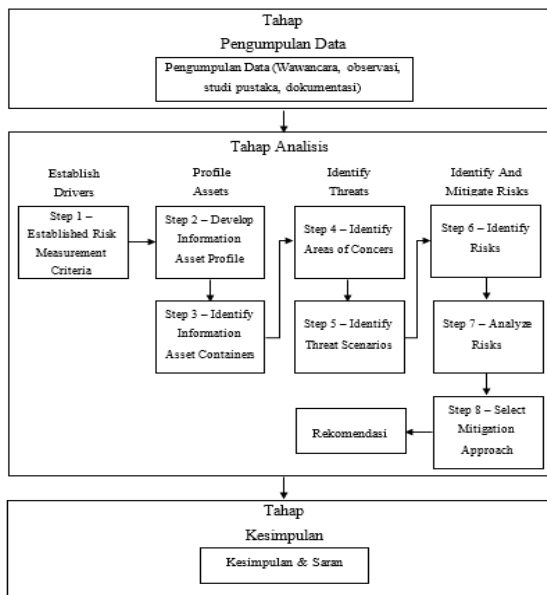
Universitas Amikom Purwokerto memberikan pelayanan kepada mahasiswa dalam bentuk sistem student service center yang digunakan untuk pengelolaan akademik mahasiswa. Dalam sistem tersebut berisi tentang menu umum (pengumuman, peraturan mahasiswa, visi misi), akademik (data agenda akademik, data asisten, data KHS, data Transkrip nilai, data pengajuan, data jadwal ujian, data jadwal seminar, data bimbingan akademik, data kampus merdeka dan data

skripsi), events, perpustakaan (pengajuan pengadaan), aktivitas mahasiswa (sertifikasi kompetensi, ormawa, prestasi dan seminar), proses pembelajaran (RPS, Kontrak perkuliahan, presensi dan rincian nilai), keuangan (tagihan dan histori pembayaran) dan Lainnya (email amikom, akun wifi dan bantuan). Contoh permasalahan yang sering terjadi pada student service center adalah seringnya terjadi server error pada saat melakukan pengisian KRS online yang mengakibatkan banyaknya mahasiswa yang mendapatkan kelas acak sehingga jadwalnya bertabrakan. Selain itu pada saat sudah melakukan pengisian KRS, dan melakukan cetak kartu sering terjadi kekeliruan pada hasil isi yang telah dilakukan mahasiswa.

Jika permasalahan yang terjadi terhadap penggunaan student service center tidak diperbaiki maupun dimitigasi dengan baik maka risiko yang diperoleh akan berdampak negative terhadap Universitas Amikom Purwokerto. Dalam mengurangi risiko, mengetahui jenis risiko dan merancang mitigasi yang sesuai dengan risiko yang terjadi maka perlu adanya pengukuran risiko terhadap teknologi informasi yang digunakan (Viyanto, Latuihamallo, Tua, Gui, & Suryanto, 2013). Metode OCTAVE Allegro merupakan salah satu metode untuk melakukan pengukuran manajemen risiko (Saputra, Ambarwati, & Setiawan, 2020). OCTAVE Allegro merupakan suatu pendekatan terhadap evaluasi risiko keamanan informasi yang bersifat komprehensif, sistematis, kontekstual dan dapat dilakukan dan diarahkan sendiri (Supradono, 2009).

## II. METODE PENELITIAN

konsep penelitian yang dilakukan dalam penelitian ini digambarkan pada gambar 1.



Gambar 1. Tahapan Penelitian

Berdasarkan dari gambar 1. konsep penelitian di atas maka dijealskan sebagai berikut:

1. Tahap Pengumpulan Data
 

Pada tahap pengumpulan data ini menggunakan beberapa metode yaitu metode wawancara, observasi, studi pustaka dan dokumentasi.
2. Tahap Analisis
 

Tahap ini dilakukan dengan metode OCTAVE Allegro yang memiliki 4 fase (Caralli, Stevens, Young, & Wilson, 2007), yaitu :

  - a. Fase pertama *Establish Drivers* yang memiliki 1 proses yaitu *Establish Risk Measurement Criteria*, dimana proses ini membangun kriteria penilaian risiko yang terus menerus. Kriteria penilaian risiko digunakan agar hasil evaluasi sesuai dengan bagian area yang sudah ditentukan.
  - b. Fase kedua *Pofile Assets* yang memiliki 2 proses yaitu *develop information asset profile* dan *identify information asset containers*, dimana proses ini membuat profil aset yang akan menjadi fokus dari penilaian risiko untuk diidentifikasi dan diperjelas pada fase selanjutnya. Dalam langkah ketiga, semua *container* yang mengirim, memproses dan menyimpan baik eksternal dan internal.
  - c. Fase ketiga *Identify Asset* yang memiliki 2 proses yaitu *Identify Areas of Concern* dan *Identify Threat Scenarios*, merupakan proses identifikasi risiko mengenai kondisi

atau situasi yang memungkinkan dapat mengancam aset informasi perusahaan. Area-area yang telah diidentifikasi diperluas menjadi skenario ancaman yang lebih mendetailkan properti dengan menggunakan sebuah *threat tree*.

- d. Fase keempat *Identify and Mitigate Risks* yang memiliki 3 proses yaitu *Identify Risks, Analyze Risks, & Select Mitigation Approach*. pada proses ini konsekuensi bagi organisasi jika sebuah ancaman terjadi dicatat, dalam mendapatkan gambaran risiko secara lengkap. Terakhir organisasi menentukan risiko yang memerlukan mitigasi dan mengembangkan strategi untuk mengurangi risiko tersebut.

3. Tahap Kesimpulan

Kesimpulan merupakan gagasan yang tercapai dan diperoleh dari uraian fakta yang ada.

III. HASIL DAN PEMBAHASAN

1. Fase 1 *Establish Drivers*

Kegiatan *Establish Risk Measurement Criteria*

Analisis dan tahapan metode OCTAVE allegro yaitu membangun kriteria pengukuran risiko untuk *impact area* dan penentuan skala prioritas. Untuk *impact area* yang akan diukur disesuaikan dengan metode OCTAVE allegro yaitu: reputasi dan kepercayaan pelanggan, finansial, produktivitas, keamanan dimana *impact area* reputasi kepercayaan pelanggan seperti pada tabel 1.

Tabel 1. *Impact Area Prioritization*

<i>Allegro Worksheet 7 Priority</i>	<i>Impact Area Prioritization Worksheet Impact Area</i>
4	Reputasi Dan Kepercayaan Pelanggan
2	Keuangan
3	Produktivitas
1	Keamanan

2. Fase 2 *Profile Asset*

a. Kegiatan *Develop Information Asset Profile*

Aset kritis pada Universitas Amikom Purwokerto yaitu terdiri dari informasi, sistem informasi, *hardware, software* dan

Sumber Daya Manusia. Setelah mengidentifikasi aset kritis, selanjutnya dilakukan *profiling* aset sistem informasi *student service center* seperti tabel 2.

Tabel 2. *Critical Information Asset Profile*

Aset	Aset Kritis
<b>Informasi</b>	Database informasi Menu Umum (Pengumuman, peraturan mahasiswa, visi misi) Akademik (Data agenda akademik. Data asisten, data KHS, data Transkrip nilai, data pengajuan, data jadwal ujian, data jadwal seminar, data bimbingan akademik, data kampus merdeka dan data skripsi) Events Perpustakaan (Pengajuan pengadaan) Aktivitas Mahasiswa (sertifikasi kompetensi. Ormawa, prestasi dan seminar) Proses pembelajaran (RPS, Kontrak perkuliahan, presensi dan rincian nilai) Keuangan (Tagihan dan History Pembayaran) Lainnya (email amikom, akun wifi dan bantuan)
<b>Sistem Informasi</b>	<i>Student service center</i>
<b>Hardware</b>	PC, server, router, switch/hub, acces point wireless
<b>Sotfware</b>	Windows OS
<b>Sumber Daya Manusia</b>	Bidang IT, Bidang Laboran, Bidang BAA, Bidang Keuangan, Bidang Fakultas, mahasiswa

b. Kegiatan *Identify Information Asset Containers*

Pada langkah ini akan mengidentifikasi container terkait lokasi aset informasi yang tersimpan dan dikelola baik internal maupun eksternal. Adapun tempat penyimpanan aset informasi ini bisa berupa *technical container*, *physical container*, dan *people container*.

Tabel 3 *Information Asset Risk Environment Map*

Allegro Worksheet		Information Asset Risk Environment Map
<b>Internal</b>		
Containers Description		Owner(S)
1. <i>Module Pedoman</i>		Universitas Amikom Purwokerto
2. <i>Server</i>		Universitas Amikom Purwokerto
3. Jaringan internet internal		Universitas Amikom Purwokerto
4. Sistem Operasi Windows, Server		Universitas Amikom Purwokerto
5. Aplikasi : student service center		Universitas Amikom Purwokerto
6. <i>Hardisk External &amp; cloud</i>		Universitas Amikom Purwokerto
7. PC		Universitas Amikom Purwokerto
<b>External</b>		
Containers Description		Owner(S)
1. Perangkat jaringan		Bisnet dan Telkom

3. Fase 3 *Identify Threats*

a. Kegiatan *Identify Areas of Concern*

Pada langkah ini akan melakukan identifikasi *areas of concern*. *Areas of concern* yaitu pernyataan deskriptif yang menjabarkan kondisi atau situasi yang sebenarnya dan dapat mempengaruhi aset sistem informasi *student service center*.

Tabel 4. *Areas of Concern*

<i>Area of Concern</i>	Jenis Serangan
Pengeksploitasian celah keamanan sistem oleh pihak internal atau eksternal	a. Virus b. Trojan c. Worm d. Spyware
Kapasitas ruang penyimpanan pada server	Server bermasalah saat banyak yang akses
Internet yang tidak stabil	Pembagian akses internet kurang tepat, jalur internet yang kurang tepat, provider bermasalah

b. Kegiatan *Identify Threat Scenarios*

Pada langkah ini memperluas masing-masing *areas of concern* menjadi *threat scenarios* yang menjelaskan bagaimana sebuah tindakan atau masalah dapat menimbulkan ancaman terhadap aset

informasi dengan mengidentifikasi *properties of threat*.

Tabel 5. *Properties of threat*

Item	Keterangan
<b>Eksplorasi celah keamanan sistem</b>	
<i>Aktor</i>	Virus dll
<i>Means</i>	Gangguan yang menyebabkan <i>software defect</i>
<i>Motive</i>	Tidak Sengaja
<i>Outcame</i>	<i>Interruption, Destruction</i>
<i>Security Requirement</i>	selalu mengupdate antivirus dan penerapan wirewall yang sesuai
<i>probabilty</i>	<i>Low</i>
<b>Kapasitas ruang penyimpanan</b>	
<i>Aktor</i>	Server bermasalah saat banyak yang akses
<i>Means</i>	Gangguan yang menyebabkan sistem <i>down</i>
<i>Motive</i>	Tidak Sengaja
<i>Outcame</i>	<i>Interruption, Modification</i>
<i>Security Requirement</i>	Menambah kapasitas untuk server
<i>probabilty</i>	<i>High</i>
<b>Internet yang tidak stabil</b>	
<i>Aktor</i>	Sumber daya internal dan Provider
<i>Means</i>	Internet bermasalah
<i>Motive</i>	Tidak Sengaja dan di sengaja
<i>Outcame</i>	<i>Interruption</i>
<i>Security Requirement</i>	Tata Kelola ulang jalur jaringan, menambah provider
<i>probabilty</i>	<i>High</i>

4. Fase 4 *Identify and Mitigate Risk*

a. Kegiatan *Identify Risks*

Pada langkah ini akan ditentukan bagaimana *threat scenario* yang sudah didokumentasikan pada *Information Asset Risk Worksheet* dapat menimbulkan dampak terhadap perusahaan atau organisasi.

Tabel 6. *Information Asset Risk Worksheet Identify Risk*

Area of Concern	Concequences
Pengeksploitasian celah keamanan sistem oleh pihak internal atau eksternal	a. Kehilangan data mahasiswa b. Data mahasiswa rusak c. Proses akademik terganggu d. Proses pembelajaran terganggu e. Pelayanan terhadap mahasiswa tidak bisa

Kapasitas ruang penyimpanan pada server	a. Tidak bisa akses sistem b. Loading sistem menjadi lama c. Input data yang tidak sempurna d. Tampilan sistem tidak sesuai aslinya
Internet yang tidak stabil	a. Server sistem Tidak bisa diakses b. Loading sistem menjadi lama

b. Kegiatan *Analyze Risk*

Skenario ancaman dan konsekuensi yang sudah dibuat akan dilihat bagaimana pengaruhnya terhadap kriteria yang ada.

Tabel 7. *Information Asset Risk Worksheet Analyze Risk*

Area of Concern	Impact Area	Value	Score
Pengeksploitasian celah keamanan sistem	<i>Reputation &amp; Customer Confidence</i>	High	12
	<i>Financial</i>	low	2
	<i>Produktivity</i>	High	9
	<i>Safety</i>	Low	1
	Score		24
Kapasitas ruang penyimpanan	<i>Reputation &amp; Customer Confidence</i>	High	12
	<i>Financial</i>	Med	4
	<i>Produktivity</i>	High	9
	<i>Safety</i>	Low	1
	Score		26
Internet yang tidak stabil	<i>Reputation &amp; Customer Confidence</i>	High	12
	<i>Financial</i>	High	6
	<i>Produktivity</i>	High	9
	<i>Safety</i>	Low	1
	Score		28

c. Kegiatan 8 *Select Mitigation Approach*

Pada langkah ini akan ditentukan bagaimana tindakan pendekatan mitigasi risiko yang tepat.

Tabel 8 *Information Asset Risk Worksheet*

Area of Concern	Mitigation
Pengeksploitasian celah keamanan sistem oleh pihak internal atau eksternal	1. Update Antivirus secara rutin 2. Pemasangan Firewall

	<ol style="list-style-type: none"> <li>3. Tidak menggunakan email/data untuk hal yang tidak perlu</li> <li>4. Pembuatan SOP penanganan apabila terkena masalah keamanan sistem</li> <li>5. Mengadakan pelatihan bagi sumber daya terkait dengan keamanan sistem</li> </ol>
Kapasitas ruang penyimpanan pada server	<ol style="list-style-type: none"> <li>1. Menambah kapasitas ruang penyimpanan</li> <li>2. Pembagian waktu saat akses sistem</li> <li>3. Pembuatan SOP apabila sistem <i>down</i></li> </ol>
Internet yang tidak stabil	<ol style="list-style-type: none"> <li>1. Tata ulang jalur jaringan</li> <li>2. Ganti provider internet</li> <li>3. Menambah kapasitas bandwidth</li> <li>4. Mengatur ulang manajemen bandwidth</li> </ol>

#### IV. KESIMPULAN DAN SARAN

Dari hasil pembahasan dapat ditarik kesimpulan bahwa terdapat 3 *area of concern*. Terdapat 4 *Impact Area Prioritization* dengan urutan prioritas reputasi, produktivitas, keuangan dan keamanan. Pada *area of concern* eksploitasi celah keamanan sistem terdapat 5 mitigasi. Pada kapasitas ruang penyimpanan terdapat 3 mitigasi dan bagian internet yang tidak stabil terdapat 4 mitigasi. Dari hasil analisis risiko terdapat nilai paling tinggi yaitu 28 adalah *area of concern* internet yang tidak stabil pada sistem yang digunakan.

#### DAFTAR PUSTAKA

- Ash Siddiqi, H. I., Darwiyanto, E., & Priyadi, Y. (2023). IT Risk Management Analysis on Bank Xyz E-Banking Service System Using Iso 31000. *JIPi (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, 8(1), 211–217. <https://doi.org/10.29100/jipi.v8i1.3325>
- Asrori, M., Murtiasri, E., Raharjanti, R., & Evayanti, N. (2020). Analisis Manajemen Resiko Sistem Pembelajaran Berbasis Elektronik El-Nino di Politeknik Negeri Semarang. *Prosiding Seminar Hasil Penelitian Dan Pengabdian Masyarakat*,

498–513. Semarang.

- Atmojo, S. A., & Manuputty, A. D. (2020). Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 7(3), 546–558. <https://doi.org/10.35957/jatisi.v7i3.525>
- Caralli, R. a R. a. C., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. *Young*, (May), 1–113.
- Diansyah, R. (2019). Identifikasi Risiko Aset Informasi Pada Sistem Informasi Akademik. *Jurnal Fasilkom*, 8(1), 289–298. <https://doi.org/10.37859/jf.v8i1.1197>
- Evinia, E., & Sitokdana, M. N. N. (2023). Risk Management Based IT Analysis Using ISO 31000 (Case Study: PT Bawen Mediatama). *Journal of Information Systems and Informatics*, 5(1), 380–390. <https://doi.org/10.51519/journalisi.v5i1.420>
- Fu, C. H., & Chen, C. Y. (2021). A study on decision-making opinion exploration in windows-based information security monitoring tool development. *Sustainability (Switzerland)*, 13(7). <https://doi.org/10.3390/su13073815>
- Ichsan, R., Falach, A., Abdurrahman, L., Santoso, I., & Si, S. (2021). *Octave Allegro Risk Analysis And Information Security Control Design In Hospital Management Information System Billing Module Using Octave Allegro*. 8(2), 2709–2722.
- Prabowo, W. S., . W., A Setiawan, N., Muslim, M. H., & Utama, Y. S. (2017). Manajemen Risiko Infrastruktur Cloud Pemerintah Menggunakan Nist Framework Studi Kasus Lembaga Ilmu Pengetahuan Indonesia (LIPI). *Jurnal Penelitian Pos Dan Informatika*, 7(1), 17. <https://doi.org/10.17933/jppi.2017.070102>
- Saputra, R. R., Ambarwati, A., & Setiawan, E. (2020). Manajemen Risiko Teknologi Informasi Menggunakan Octave Allegro Pada Pt.Hd. *Jurnal Sains, Teknologi Dan Industri*, 17(1), 1. <https://doi.org/10.24014/sitekin.v16i2.7457>
- Sari, D. K., Sakethi, D., Prabowo, R., Komputer, J. I., & Lampung, U. (2019). © 2019 Ilmu Komputer Unila Publishing

- Network all right reserve Jurnal Komputasi* Pengembangan Sistem Pencarian Pada Tujuh Kitab Hadis Pendahuluan © 2019 Ilmu Komputer Unila Publishing Network all right reserve Metodologi Tahapan Penelitian *Jurnal Komputas.* 7(1), 27–34.
- Setiawan, I., Sekarini, A. R., Waluyo, R., & Afiana, F. N. (2021). Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, 20(2), 389–396.  
<https://doi.org/10.30812/matrik.v20i2.1093>
- Supradono, B. (2009). Manajemen risiko keamanan informasi dengan menggunakan metode octave (operationally critical threat, asset, and vulnerability evaluation). *Media Elekrika*, 2(1), 4–8.
- Syihabuddin, A., Suryanto, Y., & Salman, M. (2019). Risk Management in Data Centers Using ISO 31000 Case Study: XYZ Agency. *THE 1st STEEEM 2019*, 1(1), 341–352.
- Viyanto, A. R., Latuihamallo, O. S., Tua, F. M., Gui, A., & Suryanto, S. (2013). Manajemen Risiko Teknologi Informasi: Studi Kasus pada Perusahaan Jasa. *ComTech: Computer, Mathematics and Engineering Applications*, 4(1), 43.  
<https://doi.org/10.21512/comtech.v4i1.2682>