KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 5, No. 2, April (2024), pp. 405-413

Penilaian Manajemen Risiko Menggunakan Octave Allegro Pada Data Center Perguruan Tinggi

Fitriadi Nurdin
Universitas Terbuka, Indonesia
E-mail: fitriadi@ecampus.ut.ac.id

Abstract

An organization can prevent a risk from occurring by taking planning or mitigation steps that must be taken if an error occurs so that it does not have a negative impact on the organization's activities. The data center is the heart of the information technology infrastructure owned by XYZ University because there needs to be risk management in place if a threat occurs whether from within or from outside. Three security factors that must be protected in an information security system are confidentiality, integrity and availability. The absence of a risk analysis made by XYZ University has resulted in the absence of mitigation steps that must be taken if a threat or failure occurs in the Data Center. Based on the results of risk management research using OCTAVE Allegro carried out at XYZ University, 9 important information assets were produced, of which 5 assets must be mitigated, namely errors during network maintenance in the server room, service interruption due to power failure, internet connection disruption, damage to server hardware, Natural disasters that result in damage to related devices, and 4 information assets must be postponed, namely leaking of access rights such as administrator username and password, server space being accessed by unauthorized parties, bugs/errors during system updates, exploitation of system security gaps in the server from outside parties. and in the..

Keywords: *Management, Risk, OCTAVE, Allegro, Data, Center.*

Abstrak

Suatu organisasi dapat mencegah terjadinya suatu risiko dengan melakukan Langkah perencenaan atau mitigasi yang harus dilakukan jika terjadinya suatu kesalahan sehingga tidak berpengaruh buruk terhadap kegiatan organisasi. Data center menjadi jantung dari suatu infrastruktur teknologi informasi yang dimiliki oleh Universitas XYZ oleh karena perlu adanya manajemen risiko yang dibuat jika terjadi ancaman baik yang berasal dari dalam atau dari luar. Tiga faktor keamanan yang harus mendapat perlindungan dalam sistem keamanan informasi yaitu kerahasiaan (security), integritas (integrity), dan ketersediaan (availability). Belum adanya Analisis reisiko yang dibuat oleh Universitas XYZ mengakibatkan tidak adanya Langkah mitigasi apa yang harus dilakukan jika terjadi ancaman atau kegalan pada Data Center. Berdasarakan hasil penelitian Manajemen resiko dengan Mennngunakan OCTAVE Allegro yang dilakukan pada Universitas XYZ dihasilkan 9 aset informasi penting, Dimana 5 aset harus dimitigasi yaitu Kesalahan ketika maintenance jaringan di ruang server, Terhentinya layanan karena supply listrik mati , Gangguan koneksi internet, Kerusakan pada hardware server, Bencana alam yang mengakibatkan kerusakan perangkat terkait, dan 4 aset informasi harus ditunda yaitu Bocornya hak akses seperti username dan password administrator, Ruang server diakses oleh pihak tidak berwenang, Adanya bugs/error pada saat update sistem, Eksploitasi celah keamanan sistem di server dari pihak luar dan dalam.

Keywords: *Manajemen, Risiko, OCTAVE, Allegro, Data, Center*

ISSN: 2720-992X

1. Pendahuluan

Suatu organisasi harus memeperhatikan manajemen risiko untuk menjaga serta menjamin kerahasiaan data baik internal suatu perusahaan dan pihak pelanggan, menjaga citra atau nama baik suatu organiasi sehingga tetap mendapat kepercayaan dari masyaraakat. Setiap organisasi dapat mencegah terjadinya suatu risiko dengan melakukan langkah perencanaan atau mitigasi yang harus dilakukan jika terjadi kesalahan atau kegagalan sehingga tidak berpengaruh buruk terhadap kegiatann suatu organisasi. Kemananan informasi mutlak diperhatikan untuk menghindari terjadinya kebocoran-kebocoran rahasia pengguna dan informasi-informasi penting perusahaan sesuai dengan aspek-aspek tujuan keamanan informasi yang mencangkup Confidentiality, Integrity dan Availability [1]. Informasi yang dihasilkan dapat menjadi celah keamanan yang penting untuk dijaga, Informasi penting yang jatuh ke pihak lain dapat mengakibatkan kerugian bagi pemilik informasi[2]. Sasaran utama dari penerapan manajemen risiko yaitu dapat melindungi instansi terkait dari kerugian besar yang mungkin akan muncul dan juga dapat membantu dalam menghadapi berbagai keadaan merugikan yang tidak dapat diprediksi sebelumnya [3]. Keamanan sistem informasi adalah salah satu tantangan terbesar yang harus dihadapi oleh hampir semua organisasi di dunia saat ini[4]. Tiga faktor keamanan yang harus mendapat perlindungan dalam sistem keamanan informasi adalah kerahasiaan (security), integritas (integrity), dan ketersediaan (availability)[5].

Manajemen keamanan sistem informasi sangatlah penting bagi suatu institusi dalam pengelolaan aset informasi yang mengacu pada sebuah standar[6]. Evaluasi Sistem Informasi berarti evaluasi dibidang perangkat, hardware, software, jaringan komputer, data dan sumber daya manusia. Tujuan utama dari evaluasi sistem informasi nantinya adalah upgrade, terutama dalam perbaikan fungsi dan sistem, serta kualitas pemeliharaan mengingat investasi yang telah dilakukan[7]. Saat ini koneksi internet yang sangat bagus di dunia, hal tersebut menjadi rentan terhadap kirisis infrastruktur dengan adanya ancaman dari dunia maya, baik yang disponsori negara, kriminal ,kelompok atau individu [8].

Data Center membutuhkan perlindungan baik secara fisik maupun logis untuk mengamankan sistem informasi dari serangan keamanan. Ancaman keamanan informasi seperti pencurian informasi, penolakan layanan dan akses tidak sah dapat menyebabkan dampak buruk bagi perusahaan baik kehilangan pendapatan, reputasi dan kepercayaan dari pelanggan[9]. Universitas XYZ mempunyai Data Center yang berada pada Unit Pusat Komputer dimana dalam Gedung tersebut terdapat perangkat Server dan perangkat jaringan. Terdapat 7 server yang menampung informasi yang berasal dari data akademik mahasiswa dan data administrasi. Data center dalam pengoperasiannya tentunya akan menimbulkan ancaman yang berpengaruh proses pelayanan akademik baik kepada mahasiswa maupun kepada dosen.

Universitas XYZ merupakan Universitas yang berada di Sulawasi Barat, Universitas XYZ terdiri dari beberapa fakultas yaitu Fakultas Ekonomi, Fakultas Teknik, Fakultas Matematika dan Ilmu Pengetahuan Alam, Fakultas Keguaruan dan Ilmu Politik, Fakultas Peternakan dan Perikanan. Adapun jumlah mahasiswa sebanyak 10.573 dengan jumlah pegawai sebanyak 461. Data Center Universitas XYZ sebagai pusat penyimpanan data, Ruangan data center terdiri dari beberapa server yang berguna untuk menyimpan data seperti data Akademik mahasiswa, data Pegawai dan Dosen, data Keuangan, Web server, dan email. Pada penelitian ini analisis risiko yang digunakan dengan menggunakan metode OCTAVE Allegro. Adapun latar belakang dalam penelitian ini yaitu untuk mengetahui ancaman dan risiko yang ditimbulkan terhadap data dan informasi pada Data center dengan memberikan peringkat sesuai dengan metode OCTAVE Allegro. Hasil peringkat akan menjadi pedoman bagi pihak Universitas jika terjadi risiko yang ditimbulkan jika terjadi gangguan.. Hasil analisis risiko menggunakan metode OCTAVE Allegro ditemukan 9 area perhatian terhadap asset informasi yang dianggap paling kritis.

2. Metodologi Penelitian

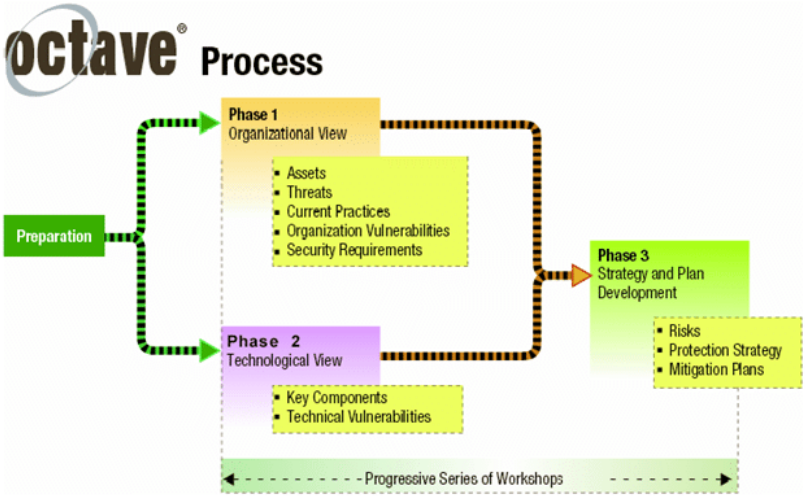
Risiko adalah kemungkinan kerugian atau kerusakan yang disebabkan oleh suatu tindakan. Risiko harus dikelola dengan baik dan terstruktur secara meneyeluruh. Manajemen risiko adalah pendekatan terstruktur untuk mengelola ketidakpastian yang terkait dengan ancaman, atau rangkaian aktivitas manusia, termasuk penilaian risiko, mengembangkan strategi untuk mengelola mitigasi dan risiko dengan menggunakan pemberdayaan/manajemen sumber daya. Strategi yang ditempuh yaitu membagi risiko kepada pihak lain, menghindari risiko, mengurangi efek negatif risiko, dan menampung sebagian atau seluruh risiko dari konsekuensi tertentu [10].

Manajemen risiko adalah proses berulang yang membahas analisis, perencanaan, implementasi, pengendalian dan pengawasan kebijakan dan langkah-langkah implementasi kebijakan keamanan. Sebaliknya, penilaian risiko dilakukan pada waktu tertentu dan memberikan gambaran penilaian risiko sementara dan juga memberikan ukuran risiko proses manajemen [11].

OCTAVE memberikan pandangan terhadap risiko teknologi informasi dalam konteks organisasi secara luas, menggambarkan kondisi pada rentan waktu tertentu sebagai dasar yang dapat digunakan untuk menyiapkan fokus mitigasi dan penigkatan kualitas [11]. OCTAVE framework Merupakan versi OCTAVE yang paling pertama, dimana pelaksanaannya dengan cara mengadakan serangkaian workshop yang difasilitasi oleh team analis multi disiplin yang berasal dari berbagai komponen unit bisnis (senior majamen, IT, manajer operasional, staf, dll).

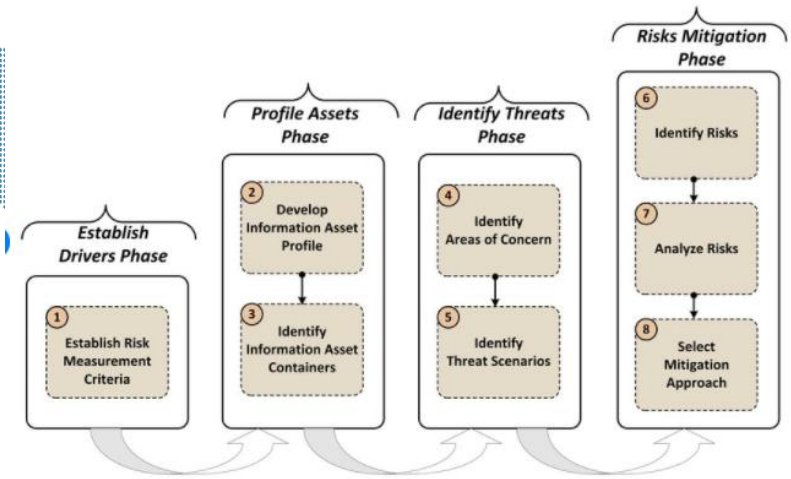
Metode ini di desain untuk perusahaan/organisasi besar yang memiliki lebih dari 300 personil serta memiliki karakter sebagai berikut :

1. Memiliki multi level hierarki.
2. Mengurus infrastruktur IT sendiri.
3. Memiliki kemampuan untuk melakukan evaluasi terhadap kerentanan.
4. Memiliki kemampuan untuk menginterpretasikan hasil dari evaluasi terhadap kerentanan.



Gambar 1. Tahapan OCTAVE Framework [12]

OCTAVE Allegro merupakan metode yang menggunakan pendekatan OCTAVE dan dirancang untuk melakukan penilaian risiko terhadap operasional organisasi dengan tujuan menghasilkan hasil yang lebih kuat tanpa perlu mendalami pengetahuan penilaian risiko yang luas. OCTAVE Allegro berbeda dengan metode OCTAVE lainnya karena metode ini berfokus pada aset informasi dalam organisasi atau perusahaan dalam lingkup bagaimana aset tersebut digunakan, dimana aset tersebut disimpan, dibawa, dan diproses, dan bagaimana aset tersebut terkena ancaman, kerentanan, dan gangguan. Metode ini terdiri dari delapan tahap yang disusun dalam empat fase (R.A. Caralli et al., 2007) .



Gambar 2. Tahap dan Langkah OCTAVE Allegro [13]

3. Hasil dan Pembahasan

Penelitian ini dilakukan dengan melakukan pengamatan serta wawancara langsung ke Universitas XYZ bagian Teknologi Informasi dan Komunikasi yang terkait dengan Data Center. Setelah dilakukan pengamatan serta didiukung oleh data maka dilakukan peneliaian risiko dengan menggunakan OCTAVE allegro.

OCTAVE Allegro Risk Assesment

1) Langkah 1, Menetapkan Kriteria Pengukuran Risiko

Melakukan pengamatan serta wawancara Unit Pusat Komputer Universitas XYZ berdasarkan hasil wawancara dan diskusi maka dapat dapat ditentukan kriteria pengukuran risiko. Terdapat 2 kriteria pengukuran risiko langkah 1 yaitu Impact area dan penentuan skala prioritas pada impact area yang sudah ditentukan. Impact area yang dipilih yaitu dipilih adalah reputasi dan kepercayaan pelanggan, finansial, produktivitas, keamanan, kesehatan, denda dan penalti.

Tabel 1. Impact area-Reputasi dan kepercayaan Pengguna dan masyarakat

	Impact Area	Low	Moderate	Hight
Reputasi dan Kepercayaan pengguna dan masyarakat	Reputation	Reputasi Instansi berdampak minimal: tidak ada usaha untuk pemulihan.	Reputasi Instansi rusak dan perlu usaha dan biaya untuk pemulihan.	Reputasi Instansi rusak parah.
	Kepercayaan Pengguna dan Masyarakat	Kepercayaan pengguna dan masyarakat dibawah 10%	20% hingga 50% Pengurangan kepercayaan dari pengguna dan masyarakat	Lebih dari 50% Hlangnya kepercayaan dari pengguna dan masyarakat

Tabel 2. Skala prioritas impact area

Priority	Impact Areas
5	Reputasi dan kepercayaan mahasiswa
4	Keuangan
3	Produktivitas
2	Keselamatan dan kesehatan
1	Tuntutan Hukum

2) Langkah 2, Membuat Profil Aset Informasi

Langkah 2 : Mengembangkan Profil Aset Informasi Aset informasi terpilih adalah informasi yang berhubungan dengan atau aset penting bagi Universitas XYZ. Alasan untuk Aset informasi penting akan dicatat pada lembar kerja aset informasi penting yang telah disediakan oleh OCTAVE Allegro. Hal-hal yang perlu diperhatikan dalam pemilihan aset informasi adalah:

1. Aset informasi yang penting,
2. Aset informasi yang digunakan dalam operasional sehari-hari
3. Aset informasi yang jika hilang dapat mengganggu kegaiatan akademik pada Universitas XYZ

Dari hasil pertimbangan diatas dapat diputuskan aset yang tergolong kritis pada Data Center yaitu

Langkah 3 sampai langkah 8 menggunakan profil aset informasi yang penting dalam bentuk worksheet. Dibawah ini merupakan penejelasan menegenai asset informasi kritikal diatas, terkait dengan aspek alasan pemilihan, deskripsi, pemilik, persyaratan keamanan, dan persyaratan keamanan yang paling penting. Persyaratan keamanan terbagi lagi menjadi tiga bagian yaitu confidentiality, integrity, dan availability. Penjelasan di bawah ini merupakan hasil mapping dari information asset profiling yang telah dilakukan sebelumnya.

Tabel 3. Information asset profiling – server data akademik mahasiswa

Critical Asset		Server Data Akademik
Rationale for Selection		Informasi mengenai data mahasiswa, data dosen, data nilai mahasiswa
Description		Server yang berisi tentang system informasi akademik yang ada pada Universitas XYZ
Owner		Unit Pelaksana Teknologi Informasi dan Komunikasi
Security Requirement	*Confidentiality*	Hanya bagian Teknologi Informasi dan Komunikasi yang bisa mengakses server tersebut
	Integrity	Hanya bagian Teknologi Informasi dan Komunikasi yang bisa mengakses server tersebut
	Availability	informasi nilai harus tersedia untuk mahasiswa
Most Important Security Requirement		Integrity, Alasan: server data informasi akademik mahasiswaberisi tentang informasi data mahasiswa, data nilai dan kelulusan mahasiswa

3) Langkah 3 – Mengindentifikasi container aset informasi

Mengidentifikasikan information asset containers (kontainer yang mana aset informasi disimpan, dipindahkan, atau diproses). Menggunakan worksheet Information Asset Risk Environment Map, peneliti mengidentifikasikan kontainer dimana aset informasi berada, yang dibagi dalam tiga kategori, yaitu Technical, Physical, People.

Tabel 4. Information Asset *Risk Environment Map* – Data Akademik mahasiswa

Information Asset Risk Environment Map (Technical)	
Internal	

Container Description	Owner(s)
Server : Data Akademik	Pusat Komputer
Server Data nilai mahasiswa	
External	
Container description	Owner(s)
Information Asset Risk Environment Map (Physical)	
Internal	
Container Description	Owner(s)
Dosen	Dosen
Mahasiswa	Mahasiswa

4) Langkah 4 – Mengindentifikasi area yang diperhatikan

Menjabarkan pernyataan secara deskriptrif terhadap kondisi atau situasi yang sebenarnya yang berpengaruh terhadap asset informasi. Melakukan review terhadap setiap *container* yang telah didaftarkan untuk melihat *areas of concern* yang potensial.

Tabel 5. *Area of Concern* - Transaksi Nilai Mahasiswa

No	Area of concern
1	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam
2	Bocornya hak akses seperti username dan password administrator
3	Kesalahan ketika maintenance jaringan di ruang server
4	Gangguan koneksi internet
5	Kerusakan pada *hardware server*
6	Ruang server diakses oleh pihak tidak berwenang
7	Adanya bugs/error pada saat update system
8	Terhentinya layanan karena supply listrik mati
9	Bencana alam yang mengakibatkan kerusakan perangkat terkait

5) Langkah 5 – Mengindentifikasi Skenario Ancaman

Pada langkah 5, membuat identifikasi dari ancaman dengan memberikan property dari setiap ancaman actor, means, motives, outcome dan security untuk setiap area yang diperhatikan

Tabel 6. *Properties of Threat* - Eksploitasi celah keamanan sistem di *server* dari pihak luar atau dalam

No	*Area of concern*	*Threat Properties*	
1	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam	*1.Actor*	Tidak diketahui
		2. Means	Percobaan login (*bruteforce attack*) *Password cracking*
		3. Motives	Secara sengaja
		4. Outcome	Interuption
		5. Security Requirement	Melakukan *update securty server*
2	Bocornya hak akses seperti username dan password administrator	*1.Actor*	Tidak diketahui
		2. Means	Percobaan login *(bruteforce attack) Password cracking*
		3. Motives	Secara sengaja
		4. Outcome	Interuption
		5. Security Requirement	Kebijakan standar keamanan password

6) Langkah 6 – Mengenditifikasi Risiko.

Mengidentifikasi dampak high (tinggi) , medium, dan low untuk universitas dan menghitung relative risk score. Relative risk score digunakan untuk menganalisis risiko dan membantu organisasi memutuskan strategi terbaik dalam menghadapi risiko. Score diperoleh melalui perkalian priority dengan value dari impact area. Tujuan dari langkah ini menentukan bagaimana threat scenario yang telah dicatat dapat memberikan dampak bagi perusahaan. Tabel dibawah ini merupakan cara melakukan perhitungan score :

Tabel 7. Indentifikasi Nilai Dampak

Impact area	Priority	Low	Moderate	high
Reputasi dan kepercayaan pelanggan	5	5	10	15
Finansial	4	4	8	12
Produktifitas	3	3	6	9
Keamanan dan Kesehatan	2	2	4	6
Denda dan Penalti	1	1	2	3

7) Langkah 7 – Menganlisis Risiko

Dilakukan dengan melakukan review risk measurement criteria yang telah ditetapkan pada langkah 1. Mulai dengan risk worksheet yang pertama, lakukan review dari pernyataan konsekuensi yang telah dicatat. Dan dilakukan perhitugan relative risk score yang akan digunakan untuk menganalisa risiko dan membantu organisasi untuk memutuskan strategi terbaik menghadapi risiko.

Tabel 8. Analisis Risiko – Eksploitasi celah keamanan sistem di server

No	Area Of Concern	Risk			
1	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam oleh staff Bagian Dikjar fakultas atau oleh dosen	Consequences	Informasi yang dimodifikasi menyebabkan kerusakan mengganggu validitas informasi tersebut		
		Severity	Impact Area	Value	Score
			Reputasi dan kepercayaan pelanggan	Mod	10
			Finansial	Low	4
			Produktivitas	High	9
			Keamanan dan Kesehatan	Low	2
			Denda dan penalti	low	1
			Relative score		26

8) Langkah 8 – Memilih pendekatan mitigasi

Tabel 9. *Matriks Risk* Relatif

Risk Relative Matrix		
Risk score	POOL	Mitigation Approach
30-45	1	Mitigate
16-29	2	Defer
0-15	3	Accept

Berdasarkan pada tabel *Risk Relative Matrix*, maka pendekatan mitigasi akan ditentukan untuk tiap risiko. Jika nilai skor risiko antara 0 sampai 15 maka risiko tersebut bisa diterima. Nilai Skor antara 16 sampai 29 maka risiko tersebut dimitigasi atau bisa ditangguhkan. Jika nilai risiko antara 30 sampai 45 maka risiko tersebut harus dimitigasi. Hasil lengkap pendekatan mitigasi risiko seperti terlihat pada tabel.

Tabel 10. *Hasil Analisis OCTAVE Allegro*

Area Perhatian	Action
Kesalahan ketika maintenance jaringan di ruang server	*Mitigate*
Terhentinya layanan karena supply listrik mati	*Mitigate*
Gangguan koneksi internet	*Mitigate*
Kerusakan pada hardware server	*Mitigate*
Bencana alam yang mengakibatkan kerusakan perangkat terkait	*Mitigate*
Bocornya hak akses seperti username dan password administrator	*Defer*
Ruang server diakses oleh pihak tidak berwenang	*Defer*
Adanya bugs/error pada saat update sistem	*Defer*
Eksploitasi celah keamanan sistem di server dari pihak luar dan dalam	*Defer*

4. Kesimpulan

Analisis risiko menngunakan OCTAVE Allegro akan menghasilkan profil aset, identifikasi area yang harus diperhatikan, identifikasi dan mitigasi risiko. Namun hasil mitigasi risiko masih sederhana sehingga membutuhkan analisis untuk meperioritaskan asset informasi atau area risiko yang harus dimitigasi terlebih dahulu. Berdasarkan hasil analisis risiko menggunakan OCATVE Allegro yang dilakukan pada Universitas XYZ dihasilkan 9 aset informasi penting, Dimana 5 aset harus dimitigasi yaitu Kesalahan ketika maintenance jaringan di ruang server, Terhentinya layanan karena supply listrik mati , Gangguan koneksi internet, Kerusakan pada hardware server, Bencana alam yang mengakibatkan kerusakan perangkat terkait, dan 4 aset informasi harus ditunda yaitu Bocornya hak akses seperti username dan password administrator, Ruang server diakses oleh pihak tidak berwenang, Adanya bugs/error pada saat update sistem, Eksploitasi celah keamanan sistem di server dari pihak luar dan dalam.

Daftar Pusataka

[1] I. M. M. Matin, A. Arini, and L. K. Wardhani, "Analisis Keamanan Informasi Data Center Menggunakan Cobit 5," *J. Tek. Inform.*, vol. 10, no. 2, pp. 119–128, 2018, doi: 10.15408/jti.v10i2.7026.

[2] B. Rahardjo, *Keamanan Perangkat Lunak*. PT Insan Infonesia, 2016.

[3] O. Arifudin, U. Wahrudin, and F. D. Rusmana, *MANAJEMEN RISIKO*. Widina, 2020.

[4] D. M. Alghazzawi, S. H. Hasan, and M. S. Trigui, "Information Systems Threats and Vulnerabilities," *Int. J. Comput. Appl.*, vol. 89, pp. 25–29, 2014.

[5] M. E. Whitman and H. J. Mattord, "Management of information security," *Cengage Learn.*, 2013.

[6] Syafrinal and Agusrijar, "Audit Keamanan Sistem Informasi Pada Data Center Menggunakan Standar SNI-ISO 27001," *Audit Keamanan Sist. Inf. Pada Data Cent. Menggunakan Standar SNI-ISO*, vol. 4, no. September, p. 581, 2020.

[7] F. Nafisah, W. Putra, and A. Herlambang, "Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 6, pp. 1858–1865, 2020, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/7441.

[8] N. Tariq *et al.*, "The security of big data in fog-enabled iot applications including blockchain: A survey," *Sensors (Switzerland)*, vol. 19, no. 8, pp. 1–33, 2019, doi: 10.3390/s19081788.

[9] D. Achmadi, Y. Suryanto, and K. Ramli, "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center," *Inst. Electr. Electron. Eng.*, 2018, doi: 10.1109/IWBIS.2018.8471700.

[10] J. S. Suroso and B. Rahaldi, "Risk is the possibility of loss or damage caused by an act. Risk must be managed properly and thoroughly structured.," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1306, no. Implementation In IT Governance For Support Business Strategy, pp. 92–96, 2017.

[11] C. Alberts and A. Dorofee, *Introduction to the OCTAVE Approach*, no. August. Pittsburgh, PA 15213-3890: Carnegie Mellon University, 2003.

[12] C. Woody, *Applying OCTAVE: Practitioners Report*. Carnegie Mellon University, 2006.

[13] R. A. 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.