Jurnal ICT : Information Communication & Technology
Vol. 18, No.2, Desember 2019, pp.123-129
p-ISSN: 2302-0261, e-ISSN: 2303-3363, DOI: 10.36054/jict-ikmi.v18i2.42

Risk Assessment Menggunakan Pendekatan *Octave Allegro* (Studi Kasus: Schoology.com)

Soetam Rizky Wicaksono[1*], Cataryna Lenny Dwi Rizka[2], Gracecilla Aprillia Immanuel[3]
[1,2,3]Program Studi Sistem Informasi, Universitas Ma Chung, Indonesia
Email: [1]soetam.rizky@machung.ac.id, [2]321610008@student.machung.ac.id,
[3]321610009@student.machung.ac.id

INFORMASI ARTIKEL

Histori artikel:

Naskah masuk, 30 Juni 2019
Direvisi, 30 Juli 2019
Diiterima, 31 Desember 2019

Kata Kunci:

OCTAVE Allegro
Schoology
Manajemen Risiko
Sistem Informasi

ABSTRAK

Abstract- Risk in information system, whether it is in desktop application or web commonly being ignored. Especially for public web which already having vast users. One of it is Schoology.com which has claimed themselves already having millions of users. This research discussed about the risk assesment of information systems by using the Octave Allegro approach in in the form of a possibility threat that occur in the Schoology.com site. We choose the Octave Allegro because it one of agile, fast and has the ability to provide strong risk assessment results, with relatively small investments in time and resource even for organizations that do not have extensive risk management expertise. After doing the research, the main impact areas that found on the Schoology.com are reputation and customer confidence. The results show that the level on the Schoology site is a medium because, the data contained on this site is not too important so the possibility of being misused by foreigners can be considered small.

Abstrak- Risiko dalam suatu sistem informasi kerap diabaikan, baik sistem berbasis desktop maupun web. Khususnya untuk web yang bersifat publik dan diakses secara luas. Salah satu web tersebut adalah Schoology.com yang mengklaim telah memiliki jutaan pengguna. Penelitian ini membahas tentang penerapan *risk assessment* pada sistem informasi dengan menggunakan pendekatan Octave Allegro pada salah satu kasus berupa ancaman yang mungkin terjadi pada situs Schoology.com. Metode Octave Allegro dipilih, karena salah satu metode yang dianggap *agile* dan cepat, dan telah terbukti bahwa metode risk assessment dengan menggunakan Octave Allegro memiliki kemampuan untuk memberikan hasil yang baik, dengan investasi yang relatif kecil dalam hal waktu dan sumber daya, bahkan untuk organisasi yang tidak memiliki keahlian manajemen risiko yang baik. Pada hasil penilaian terbagi ke dalam 3 tingkatan yaitu low, moderate dan high. Setelah dilakukan penelitian, impact area utama yang terdapat pada website Schoology.com yaitu reputation and customer confidence (Reputasi dan Kepercayaan Customer). Hasil menunjukkan tingkatan pada situs Schoology yaitu medium sebab, data yang terdapat pada website ini terbilang tidak terlalu penting sehingga kemungkinan untuk disalahgunakan oleh orang asing dapat dibilang kecil.

Jurnal ICT : Information Communication & Technology p-ISSN: 2302-0261
Vol. 18, No.2, Desember 2019, pp.123-129 e-ISSN: 2303-3363

***Penulis Korespondensi**:*

Soetam Rizky Wicaksono
Program Studi Sistem Informasi,
Universitas Ma Chung
Villa Puncak Tidar N-01 Malang, Jawa Timur, Indonesia
Email: soetam.rizky@machung.ac.id

1. Pendahuluan

Schoology.com merupakan salah satu sosial media yang juga dapat digunakan untuk media pembelajaran. Situs ini dibuat oleh Jeremy Friedman, Ryan Hwang, dan Tim Trinidad mahasiswa di Washington University di St. Louis, MO yang kemudian dirilis pada bulan Agustus tahun 2009. Website ini memiliki beberapa fitur yaitu c*ourses* (kursus), *groups* (kelompok), dan *resources* (sumber belajar). Selain itu pada situs ini juga ada catatan kehadiran, serta penilaian pada tes dan kuis online [1]. Schoology menjadi lebih cepat populer dibanding pesaingnya karena memiliki fitur yang mirip dengan media sosial seperti twitter dan facebook [2]. Hal ini memudahkan para guru dan siswa dalam berinteraksi serta dianggap lebih mampu meningkatkan motivasi belajar di luar kelas konvensional [3], [4]. Akibatnya, schoology memiliki pengguna yang selalu bertumbuh dan meski relatif masih muda usianya telah mampu bersaing dengan rivalnya seperti Edmodo. Namun demikian, dengan pengguna yang lebih banyak berasal dari siswa level dasar hingga menengah serta guru yang notabene bukan berasal dari latar belakang TI, maka risiko penggunaan schoology menjadi cukup besar.

Risiko dalam penggunaan schoology, dipandang sebagai sebuah sistem informasi berbasis web wajib dipertimbangkan secara seksama. Sebab dengan memahami risiko yang mungkin bisa ditimbulkan, maka pengguna dapat lebih berhati-hati serta menghindari efek negatif yang mungkin terjadi. Di sisi lain, pihak pengelola schoology juga mampu mendapat masukan mengenai risiko tersebut, sehingga mampu mengadakan perbaikan di kemudian hari.

Pendekatan manajemen risiko dalam konteks sistem informasi dapat dilakukan dengan berbagai standar ataupun metode. Pada umumnya, metode pendekatan tersebut dipilih bukan karena tingkat kerumitan atau kompleksitas yang didapat, namun lebih karena kesederhanaan pengukuran [5]. Tingkat kesuksesan pengukuran risiko bukan didapat dari hasil kompleksitas, tetapi lebih berdasarkan cara pengukuran dengan pendekatan yang sederhana serta hasil yang dapat dipahami oleh pengguna maupun pengembang sistem [6].

Salah satu pendekatan dalam pengukuran manajemen risiko yang dianggap sederhana namun dianggap sukses adalah *Octave Allegro*. Metode penilaian risiko dengan menggunakan metode *Octave Allegro* memiliki kemampuan untuk memberikan hasil yang mumpuni dengan investasi yang relatif kecil, bahkan untuk organisasi yang tidak memiliki keahlian manajemen risiko yang luas [6], [7]. Sehingga pendekatan ini dianggap sesuai dalam konteks penelitian ini.

Berdasarkan penelusuran hingga penelitian ini selesai dilakukan, belum ditemukan peneliti lain yang telah membahas topik *Octave Allegro* dengan studi kasus Schoology. Sehingga penelitian ini diharapkan dapat membantu pemahaman mengenai penerapan metode *Octave Allegro*, sekaligus memahami risiko di website Schoology.

2. Metode

Risiko dapat dikatakan sebagai indikasi bahaya terhadap seseorang atau sesuatu, juga bisa dikatakan sebagai hal potensial yang dapat terjadi pada suatu peristiwa dan mengakibatkan hal negatif didalamnya [5]. Namun demikian, risiko adalah suatu kemungkinan yang dapat dihindari jika mampu melakukan manajemen risiko yang baik.

Octave adalah metodologi untuk menyelidiki serta melakukan evaluasi risiko keamanan informasi [6]. Hal ini ditujukan untuk mendukung organisasi dalam melakukan pengembangan kriteria dalam penilaian risiko secara kualitatif sehingga dapat menampilkan toleransi risiko untuk kepentingan operasional organisasi, melakukan identifikasi aset terpenting, serta melakukan investigasi terhadap kerentanan ataupun ancaman yang mungkin bisa terjadi pada aset tersebut sekaligus mengevaluasi hal potensial yang dapat terjadi bagi organisasi [6], [8].

Kerangka kerja konseptual dari pendekatan *Octave* pada awalnya diterbitkan oleh Software Engineering Institute (SEI) di Carnegie Mellon University pada tahun 1999 [6]. Octave melakukan penilaian risiko dengan asumsi pada tiga prinsip dasar administrasi keamanan, yaitu: 1) kerahasiaan, 2) integritas, dan 3) ketersediaan sistem.

Metode *Octave* memiliki tiga perkembangan yaitu , *Octave, Octave -S. Octave Allegro* [6]. *Octave Allegro* tidak dimaksudkan untuk

menggantikan metode *Octave* yang sebelumnya tetapi merupakan metode yang dapat saling melengkapi serta menjadi yang metode terbaru. Fokus utama dari *Octave Allegro* adalah pada aset informasi yang terdapat dalam sistem. Sehingga penggunaan di dalam konteks ini yaitu bagaimana informasi tersebut digunakan, serta bagaimana informasi tersebut disimpan, diangkut serta diproses. dan bagaimana keadaannya jika terkena suatu ancaman dan gangguan sebagai dampak yang ditimbulkan. Selain itu yang termasuk dalam lampiran Octa*ve Allegro* didukung dengan panduan lembaran kerja berupa kuesioner [9].

Octave merupakan sebuah teknik dan metode yang digunakan sebagai kerangka kerja yang nantinya dapat digunakan untuk mengidentifikasi, menganalisis serta melakukan pengawasan terhadap pengelolaan risiko keamanan suatu informasi berdasarkan tahap pengidentifikasian risiko [9].

Penilaian risiko menggunakan Octave juga telah diuji secara empiris pada aset penelitian sebelumnya, hal ini ditunjukkan dengan kesamaan hasil penelitian dari dua penelitian sebelumnya yang menyatakan bahwa setiap aset informasi yang kritis menentukan batasan yang jelas. Selanjutnya aset informasi yang kritis tersebut dapat mengidentifikasi keamanan aset, sehingga dapat menentukan langkah pemenuhan skenario [9], [10].

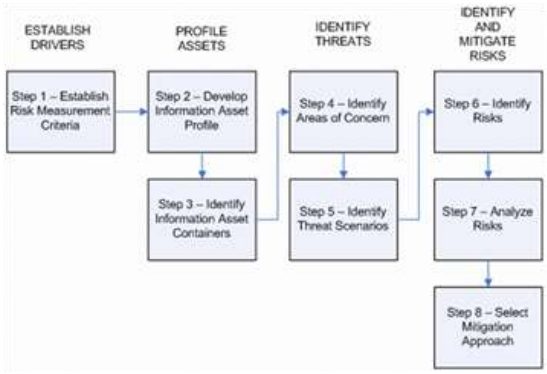
Berdasarkan hasil analisa risiko pada kedua hasil penelitian dapat diperoleh kesimpulan yang menunjukkan bahwa keamanan pada sistem informasi yang diterapkan masih kurang dan masih ditemukan banyak risiko yang diakibatkan oleh penyebab yang berbeda-beda. Oleh sebab itu digunakan metode Octave untuk menganalisis risiko keamanan sistem informasi pada IT dan dapat memberikan kemudahan dalam menindak lanjuti risiko-risiko yang nantinya mungkin akan terjadi .

Penelitian terdahulu ini digunakan sebagai salah satu panduan penulis dalam melaksanakan penelitian sehingga dapat menambah wawasan mengenai teori yang digunakan untuk mengkaji penelitian yang dilakukan. Penulis mengambil beberapa penelitian sebagai referensi dalam menambah bahan yang dikaji dalam penelitian penulis. Berikut merupakan beberapa penelitian terdahulu dalam bentuk jurnal terkait dengan proses penelitian yang telah dilakukan penulis terdahulu [13].

3. Pembahasan dan Diskusi

Langkah melakukan penilaian manajemen risiko menggunakan metode Octave Allegro pada Schoology.com, terbagi pada delapan tahapan. Tahapan tersebut tercantum pada gambar 1. Di dalam tahapan tersebut terdapat empat bagian yakni: (1) penentuan kriteria risiko, (2) profil aset, (3) identifikasi ancaman serta (4) identifikasi dan mitigasi risiko [11].

Pada tahapan pertama, dilakukan identifikasi kriteria risiko pada Schoology. Berdasarkan analisis tahapan pertama, didapatkan dua area yang paling berpengaruh yakni reputasi dan risiko kehilangan pengguna. Area pertama, yakni reputasi, didasarkan pada persaingan usaha Schoology dengan situs sejenis yang menawarkan layanan sama, seperti Edmodo ataupun *Google Classroom*. Selain itu, karena dari segi usia, Schoology termasuk yang paling muda, maka reputasi menjadi hal yang sangat berpengaruh dalam konteks ini. Area kedua yakni kehilangan pengguna atau *customer lost*, menjadi titik tumpu dalam kriteria karena pengguna Schoology dari kalangan siswa merupakan golongan yang rentan berganti ke sistem lain jika terjadi hal negatif yang tidak diinginkan. Sehingga hal ini selayaknya menjadi perhatian utama dalam penanganan risiko.



Gambar 1. Langkah Metode Octave Allegro [6], [11]

Dalam penelitian ini, hanya digunakan *worksheet* 1, 7, 8, dan 10 karena hanya *worksheet* yang bersesuaian dan berkaitan dengan studi kasus yang diambil yaitu Schoology.com. Pengukuran risiko dilakukan pada tanggal 29 Maret 2019 dan tanggal 25 April 2019.

Berdasarkan tabel 1, berikutnya masing-masing area dibagi ke dalam 3 tingkatan yaitu *low, moderate dan high*. Semakin rendah tingkatan di tiap area maka menandakan bahwa semakin tinggi reputasi dan kepercayaan pengguna.

Langkah berikutnya adalah memetakan tiap area berdasarkan tingkat kepentingan yang dilakukan. Pada penelitian ini, risiko *finance, productivity, safety and health* hingga *user defined* tidak bisa dilakukan pengukurannya, sebab hal tersebut harus dilakukan jika peneliti berada di dalam perusahaan, bukan sebagai pengguna. Sehingga berikutnya pemetaan tingkat kepentingan dapat dijelaskan di tabel 2.

Tabel 1. *Risk Measurement Criteria – Reputation and Customer Confidence*

Allegro Worksheet 1	***RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE***		
Impact Area	*Low*	*Moderate*	*High*
Reputation	Reputasi antara para pesaing memiliki dampak minimal: kecil atau tidak ada usaha sama sekali untuk pemulihan.	Reputasi antar pesaing rusak.	Reputasi antara pesaing sangat rusak.
Customer Losts	Kepercayaan yang dimiliki pengguna terhadap situs sangat tinggi karena tidak ada risiko dalam aset yang dimiliki perusahaan.	Kepercayaan pengguna terhadap situs rendah terhadap risiko dalam aset instansi tersebut.	Kepercayaan pengguna kepada situs hilang karena risiko yang ditimbulkan terhadap aset perusahaan.

Tabel 2. Impact Area Prioritization Worksheet [15]

Allegro Worksheet 7	***IMPACT AREA PRIORITIZATION WORKSHEET***
Priority	*Impact Areas*
1	*Reputation and Customer Confidence*
6	*Financial*
2	*Productivity*
5	*Safety and Health*
4	*Fines and Legal Penalties*
3	*User Defined*

Tabel 3. *Critical Information Asset Profile*

Allegro Worksheet 8	***CRITICAL INFORMATION ASSET PROFILE***	
(1) Critical Aset *What is the critical information asset?*	***(2) Rationale for Selection*** *Why is this information asset important to the organization?*	***(3) Description*** *What is the agreed-upon description of this information asset?*
Server utama	Karena di sini server berfungsi sebagai pusat semua data yang diperoleh serta dihasilkan dari *database* yang terdapat pada komputer *user* yang terhubung.	Pengamanan data rahasia dari semua tabel master dan kegiatan / transaksi *user*.
(4) Owner(s) *Who owns this information asset?*		
Bagian IT dari organisasi / perusahaan, yaitu Schoology.com		
(5) Security Requirements *What are the security requirements for this information asset?*		
Confidentiality	*Only authorized personnel can view this information asset, as follows:*	Bagian IT khusus, Manajer IT
Integrity	*Only authorized personnel can modify this information asset, as follows:*	Bagian IT khusus, Manajer IT
Availability	*This asset must be available for these personel to do their jobs, as follows:*	Bagian *Staff* IT
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
‰*Confidentiality*	‰ *Integrity*	✓*Availability*

Tabel 4. *Information Aset Risk Worksheet*

Allegro Worksheet 10	***INFORMATION ASSET RISK WORKSHEET***			
Information Aset (Aset Informasi)	Data *profile* dan transaksi/kegiatan *user*			
Area of Concern	Rusaknya data *user* karena terjadi perusakan sistem dari dalam.			
Threat	*(1) Actor* (Aktor) *Who would exploit the area of concern or threat?* (Siapa yang melakukan *area of concern* atau ancaman?)	*Hacker* dari luar perusahaan.		
	(2) Means *How would the actor do it? What would they do?* (Bagaimana cara aktor melakukannya?)	Mengeksekusi *malicious code* untuk dapat masuk dan merusak sistem Schoology.com.		
	(3) Motive (Motif) *What is the actor's reason for doing it?* (Apa alasan aktor melakukannya?)	Keinginan untuk merusak dan menjatuhkan perusahaan, karena persaingan atau mungkin iseng.		
	(4) Outcome *What would be the resulting effect on the information asset?* (Apa dampaknya terhadap aset informasi?)	‰ Disclosure ✓Modification ✓Destruction ✓Interruption		
	(5) Security Requirements *How would the information asset's security requirements be breached?* (*Security requirements* apa yang dilanggar?)	Hanya pihak tertentu yang mempunyai kode akses ke dalam sistem, salah satunya data *user*.		
	(6) Probability (Probabilitas) *What is the likelihood that this threat scenario could occur?* (Bagaimana kemungkinan terjadinya skenario ancaman ini?)	*‰High*	*✓Medium*	*‰Low*
Information Asset Risk	*(7) Consequences* (Konsekuensi) *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* (Apa konsekuensi yang dihadapi organisasi pemilik aset sebagai hasil dari penerobosan s*ecurity requirements*?)	*(8) Severity* *How severe are these consequences to the organization or asset owner by impact area?* (Seberapa parah konsekuensi tersebut terhadap organisasi dan pemilik aset berdasarkan *impact area*?)		

	Impact Area	***Value***	***Score***
Pelanggaran privasi karena kebocoran data *user*, yang memungkinkan disalahgunakan oleh pihak yang kurang bertanggung jawab.	*Reputation & Customer Confidence* (Reputasi dan Kepercayaan *Customer*)	*High*	15
	Financial	*Low*	2
Kerusakan sistem yang nantinya dapat berdampak pada kegiatan atau transaksi *user*.	*Productivity* (Produktivitas)	*High*	10
Dibutuhkan SDM tambahan untuk menangani masalah ini.	*Fines & Legal Penalties*	*Medium*	6
		Relative Risk Score	32

(9) Risk Mitigation
Based on the total score for this risk, what action will you take?
(Berdasarkan skor total dari risiko, tindakan apa yang akan dilakukan?)

‰Accept *‰Defer* *✓Mitigate* *‰Transfer*

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Server utama	Dilakukan pembaharuan terhadap keamanan sistem pada server utama, *update firewall* dan *anti-virus.*
Sistem administrator dan server utama	Melakukan pembaharuan *password* secara berkala.

Schoology termasuk dalam penilaian *Reputation* and *Customer Confidence* (Reputasi dan Kepercayaan Customer), karena pada situs ini terjadi kegiatan belajar dengan menggunakan media website (e-learning) untuk sekolah dan lembaga perguruan tinggi yang dapat melibatkan banyak orang di mana diperlukan kepercayaan dan kenyamanan dari customer dalam penggunaan situs ini.

Selanjutnya dilakukan pemetaan profil aset berdasarkan aset, kepemilikan serta keamanan data. Keterbatasan pemetaan profil aset dikarenakan penilaian risiko dilakukan sebagai pihak eksternal, bukan internal. Sehingga pada pemetaan keamanan, hanya ditetapkan berdasarkan dugaan, bukan pemetaan yang sesungguhnya. Sedangkan pada aset yang ditekankan pada server, tidak bisa dipetakan secara detail karena untuk lokasi serta spesifikasi server secara detail merupakan rahasia perusahaan yang tidak mungkin didapatkan di penelitian pendahuluan ini. Namun demikian, pemetaan profil aset ke bagian database merupakan penilaian subyektif, tetapi dapat dipertanggungjawabkan penilaiannya.

Berdasarkan penilaian pada tabel 3, maka dapat disimpulkan bahwa *critical aset information* dibagi ke dalam 3 bagian yaitu *critical aset, rationale for selection* dan *descriptio*n. Kemudian untuk security requirements dibagi ke dalam 3 bagian yaitu *confidentiality*, *integrity* dan *availability.* Pada bagian ini dijelaskan siapa saja yang berpartisipasi pada setiap bidang.

Sebagai pengguna eksternal, dan berdasarkan pada reputasi dan kepercayaan pelanggan, maka ketersediaan situs adalah hal yang dianggap paling penting dalam pemetaan ini. Sebab pengguna eksternal tidak memiliki akses serta pengetahuan terhadap tingkat kerahasiaan data serta integritas data. Sehingga pada saat proses registrasi pada umumnya telah memiliki tingkat kepercayaan secara penuh terhadap situs Schoology. Namun apabila situs tidak bisa diakses oleh pengguna, maka dipastikan reputasi serta tingkat kepercayaan dapat hilang seketika. Sehingga hal tersebut menjadi hal yang paling penting dalam langkah pemetaan ini.

Berdasarkan penilaian risiko pada tabel 3, maka aspek yang rentan terhadap ancaman (*threat*) dan diperlukan perhatian lebih untuk mengurangi risiko adalah sistem utama. Hal ini dikarenakan kegiatan yang dilakukan pada Schoology berbasis online (website), sehingga diperlukan peningkatan keamanan informasi agar tidak ada celah keamanan yang dapat dirusak oleh pihak luar organisasi atau perusahaan.

Pada tabel impact area terbagi menjadi 3 value, yang pertama yaitu *low* (antara 1-5), lalu yang kedua yaitu *medium* (antara 6-10) dan yang terakhir *high* (10 ke atas). Dari hasil perhitungan pada tabel 4 di dapat score 32, maksudnya adalah pada Schoology ini masih sangat mungkin terjadi ancaman dari luar perusahaan, walaupun kecil kemungkinan tetapi masih bisa terjadi. Penilaian berikut dilakukan berdasarkan pendapat peneliti.

4. Kesimpulan

Dari masing-masing impact area yang ada terbagi menjadi 3 tingkatan yaitu *low, moderate* dan *high*. Semakin rendah tingkatan setiap area maka menandakan bahwa semakin tinggi reputasi dan kepercayaan karyawan. Impact area yang menjadi prioritas dalam website Schoology merupakan Reputation and Customer Confidence (Reputasi dan Kepercayaan Customer), dikarenakan pada situs ini terjadi kegiatan belajar mengajar berbasis website (e-learning). Sehingga dapat diambil kesimpulan bahwa berdasarkan penelitian ini didapat tingkatan pada website Schoology adalah medium karena data yang tersimpan dalam website ini dapat dibilang tidak terlalu penting sehingga kemungkinan sangat kecil website ini akan disalahgunakan oleh orang asing.

Daftar Pustaka

[1] D. Schlager, "Schoology : The Adoption of a Learning Management System," 2016.

[2] C. Manning, W. Brooks, V. Crotteau, and A. Diedrich, "Tech Tools for Teachers , By Teachers : Bridging Teachers and Students," *Wisconsin English J.*, vol. 53, no. 1, pp. 24–28, 2011.

[3] A. Efendi, "E-Learning Berbasis Schoology Dan Edmodo: Ditinjau Dari Motivasi Dan Hasil Belajar Siswa Smk," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 2, no. 1, p. 49, 2017.

[4] A. S. Sicat, "Enhancing College Students' Proficiency in Business Writing Via Schoology," *Int. J. Educ. Res.*, vol. 3, no. 1, pp. 159–178, 2015.

[5] E. Wallmüller, "Risk Management for IT and Software Projects," *Bus. Contin.*, pp. 165–178, 2011.

[6] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process," *Carnegie Mellon Univ.*, no. May, p. 154, 2007.

[7] D. Ahmad Jakaria, R. Teduh Dirgahayu, and H. Magister Informatika, "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, 2013, vol. 37, pp. 1907–5022.

[8] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE ® Approach," no. August. pp. 1–27, 2003.

[9] N. Nelmiawati, F. R. Destrianto, and M. A. R. Sitorus, "Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode

OCTAVE," *J. Integr.*, vol. 9, no. 1, p. 35, 2018.
[10] Rosini, M. Rachmaniah, and B. Mustafa, "Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode OCTAVE Allegro," *J. Pustak. Indones.*, vol. 14, no. 1, pp. 14–22, 2015.
[11] PECB, "OCTAVE." PECB, 2010.