PENILAIAN RISIKO KERAWANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE ALLEGRO

Rosini[1], Meutia Rachmaniah[2], Badollahi Mustafa[3]
[1]Mahasiswa Pascasarjana IPB Program Studi Magister Teknologi Informasi untuk Perpustakaan
[2]Ketua Komisi Pembimbing, Dosen pada Departemen Ilmu Komputer FMIPA IPB
[3]Anggota Komisi Pembimbing, Dosen pada Departemen Ilmu Komputer FMIPA IPB

Abstract

This study aims to conduct risk assessment on information vulnerabilities, to get the level of information vulnerabilities, and to generate strategic recommendations to overcome information vulnerabilities in the X Library using OCTAVE Allegro as a method. The result showed that from 4 categories, information vulnerabilities at X Library is at category 3 or vulnerable enough with 22 areas of concern or equal to 42.31%. The risk assessment carried out in X Library turns the result that there are 10 assets information held by the Head of Central Library, Adminisration Services Unit, Cataloging and Classifying Unit, Circulation Services Unit, Reference Services Unit. The second result is contained threats to information assets by 52 areas of concern that conducted by internal X Library are 14 actors, by internal X are 13 actors, and by external are 2 actors. The third result is there are 62 consequences of 52 information assets with at the most consequences found in electronic document collections X-ana which from 6 areas of concern produce 10 consequences. The strategic recommendations to overcome the information vulnerabilities in X Library is adjusted according to the risk mitigation that carried out in each area of concern which is called the control or risk control. From the results of this risk assessment that can be done is to reduce or eliminate risk (mitigate) as many as 21 areas of concern, to transfer or mitigate risk as many as 16 areas of concern, to defer the risk a total of 12 areas of concern, and to receive risk (accept) or defer as much as 3 areas of concern.

Keywords: *Information Asset, Information Vulnerability, OCTAVE Allegro, Risk Assessment, threat*

Pendahuluan

Data mempunyai peran yang sangat penting dalam sebuah sistem informasi karena merupakan salah satu komponen sistem informasi selain *software, hardware, people, procedures dan networks* (Whitman & Mattord, 2012). Oleh karena itu data yang disimpan dan diproses kemudian disebarkan di dalam sistem komputer harus dilindungi keamanannya karena merupakan aset yang paling berharga dalam sebuah organisasi. Pentingnya data juga disebutkan oleh Taylor dan Joudrey (2009), yang menyatakan bahwa data digunakan sebagai dasar untuk mengambil keputusan. Data yang digunakan tersebut adalah data yang telah diorganisir menjadi suatu informasi kemudian diterima sebagai pengetahuan dan digunakan untuk mengambil keputusan.

Salah satu aspek yang harus dijaga dalam pengamanan informasi yaitu adanya kerawanan atau kerentanan (*vulnerabilities*). Perpustakaan X sebagai pusat informasi yang dipastikan banyak menyimpan informasi dan perlu segera diketahui potensi kerawanan yang muncul di perpustakaan X. Untuk itu perlu dilakukan identifikasi potensi kerawanan informasi yang ada sehingga informasi yang tersedia perpustakaan selalu mutakhir, siap dan dapat diakses dengan mudah ketika diperlukan sesuai dengan kebutuhan pemustakanya.

Metode Penilaian Risiko OCTAVE Allegro

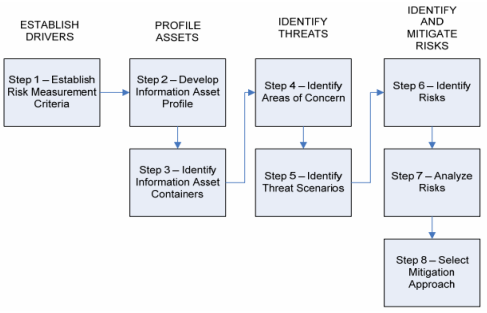
Metode OCTAVE merupakan singkatan dari t*he Operationally Critical Threat, Aset, and Vulnerability Evaluation*. Metode OCTAVE melakukan penilaian risiko berdasarkan pada tiga prinsip dasar

administrasi keamanan, yaitu: *confidentiality, integrity, availability*. OCTAVE mempunyai dua varian, yaitu OCTAVE-S dan OCTAVE Allegro. Kata allegro: (al-leg-ro) berarti dalam tempo yang cepat dan lincah. Hal ini menggambarkan kinerja OCTAVE Allegro yang lincah dan cepat. Keating (2014) menyatakan 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.

OCTAVE Allegro dapat dilakukan dalam bentuk workshop, *setting* bersama yang didukung dengan panduan, lembar kerja, dan kuesioner, yang terdapat dalam lampiran OCTAVE Allegro. 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 (Macek & Ivkovic, 2011).

Metode OCTAVE Allegro terdiri dari delapan tahap yang dikelompokkan menjadi empat kategori atau fase (Brunschwiler, 2013). Empat kategori tersebut adalah sebagai berikut:

1) Kategori 1, menetapkan apa yang menjadi arahan organisasi,
2) Kategori 2, membuat profil aset yang dimiliki organisasi.
3) Kategori 3, mengidentifikasi ancaman untuk setiap aset informasi dalam konteks wadahnya.
4) Kategori 4, mengidentifikasi dan mitigasi risiko terhadap aset informasi dan pengembangan pendekatan mitigasi.



Gambar 1. Allegro *Road Map* (Caralli *et.al.*, 2007:4).

Metode

Penelitian ini berusaha mendeskripsikan hasil kajian dari setiap tahap atau lembar kerja yang diadopsi dari metode OCTAVE allegro dalam menilai potensi kerawanan di Perpustakaan X.

Setiap tahap dari delapan tahap pada Gambar 1, dirinci lagi menjadi beberapa aktivitas penilaian risiko yang akan dilakukan (Caralli *et.al.*, 2007). Untuk memudahkan implementasinya OCTAVE Allegro memberikan panduan berupa *worksheet* 1 sampai 10 seperti di bawah ini:

Tabel 1. Rincian Tahapan Metode OCTAVE Allegro

Tahap	Aktivitas	Output	*Worksheet* /Acuan
1	Menetapkan kriteria pengukuran risiko	• Kriteria pengukuran risiko terhadap arahan organisasi • Peringkat area dampak dari yang paling penting hingga yang tidak penting	*Allegro Worksheet* 1-6 dan 7
2	Mengembangkan profil aset informasi	Profil aset informasi kritis	*Allegro Worksheet* 8

3	Mengidentifikasi *container* aset informasi	Pemetaan lingkungan risiko aset informasi	*Worksheets* 9a, 9b, dan 9c
4	Mengidentifikasi *area of concern*	Peta lingkungan risiko aset informasi	*Worksheet* 10
5	Mengidentifikasi skenario ancaman	• Informasi detail dan hasil pengembangan skenario ancaman dari *area of concern* • Daftar risiko aset informasi • Deskripsi tambahan untuk kolom 6 *worksheet*s aset informasi dan *container*	• Output tahap 4 (*Information Aset Risk Environment Maps*) • *Worksheet* 10 • *Information Aset Risk Worksheets* • *Column (6) worksheets* aset informasi dan *container*
6	Mengidentifikasi risiko	Konsekuensi dari skenario ancaman (kondisi) Tahap 6 Risiko Total = Ancaman kondisi dan konsekuensi di tahap [4 + 5] + [6]	*Information Aset Risk Worksheet*
7	Menganalisis risiko	• Tabel nilai area dampak • Tabel skor risiko	• *Risk Measurement Criteria Step 1* • *Information Aset Risk Worksheets 10*
8	Memilih pendekatan mitigasi	• Matriks risiko relatif • Tingkat kerawanan informasi • Mitigasi untuk semua daftar risiko • Strategi mitigasi untuk setiap risiko yang telah diputuskan untuk dilakukan mitigasi	

Pelaksanaan Penilaian Risiko dengan Metode OCTAVE Allegro
Tahap 1 : Menetapkan Kriteria Pengukuran Risiko

Aktivitas 1 : Mendefinisikan satu set kriteria kualitatif pengukuran risiko terhadap organisasi

OCTAVE Allegro mendaftar enam area dampak yang kemudian ditentukan nilai kualitatifnya masing-masing (rendah-sedang-tinggi). Penentuan ini berdasarkan besarnya dampak risiko yang terjadi jika KPI tidak tercapai.

Aktivitas 2 : Pembuatan skala prioritas area dampak

Urutan prioritas area dampak di Perpustakaan X dapat dilihat pada Tabel 2 di bawah ini.

Tabel 2 Urutan Prioritas Area Dampak

Prioritas	Area Dampak
1	Reputasi dan Kepercayaan Pengguna
2	Keamanan
3	Produktivitas
4	Hukum dan Peraturan
5	Keuangan atau Biaya operasional
6	Kesehatan dan Keselamatan

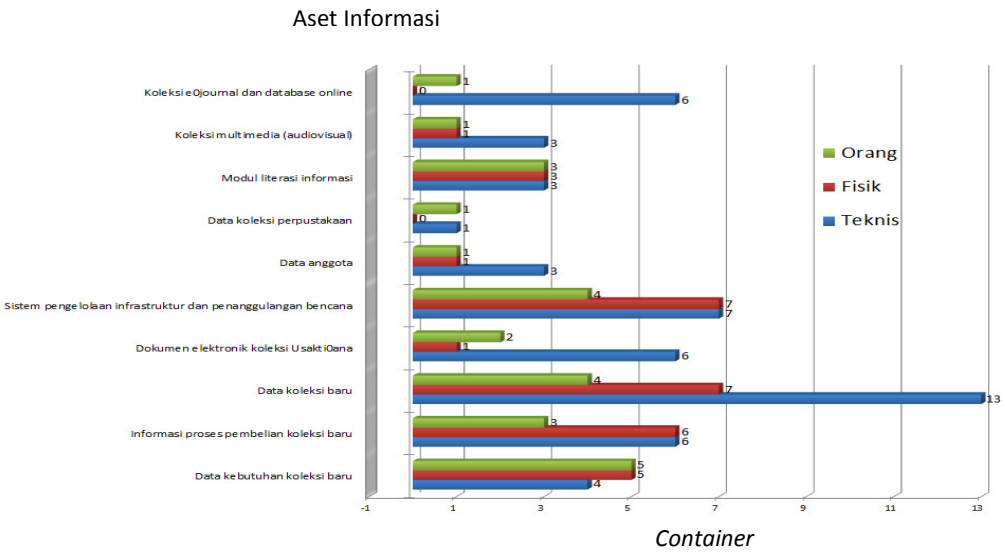
Tahap 2: Mengembangkan Profil Aset Informasi

Profil aset informasi kritis (*Critical information asets profile*) terdiri dari deskripsi aset informasi kritis itu sendiri, alasan pemilihan, dan pemiliknya (pengelola). Profil aset informasi kritis dilengkapi dengan persyaratan

(*requirements*) keamanan yang harus ada untuk melindungi aset informasi kritis tersebut dengan menyatakan kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan persyaratan keamanan lainnya, lalu dipilih persyaratan keamanan yang dianggap paling penting untuk aset informasi kritis tersebut.

Tahap 3: Mengidentifikasi C*ontainer* *A*set Informasi

Dilakukan identifikasi atau pemetaan terhadap lingkungan atau *container* aset informasi. Hasil dari pemetaan ini berupa 21 peta lingkungan aset informasi dapat dilihat pada gambar di bawah ini.



Gambar 2 Jenis dan Kategori *Container* Aset Informasi

Tahap 4 : Mengidentifikasi berbagai A*rea of Concern*

Hasil penilaian menunjukan terdapat 52 *area of concern* yang berasal dari 10 aset informasi. *Area of concern* yang terbanyak terdapat pada aset informasi Sistem pengelolaan infrastruktur dan penanggulangan bencana dengan 10 *area of concern*. Sedangkan yang paling sedikit adalah pada aset informasi Modul literasi informasi dan Koleksi *e-journal* dan *database* online.

Tahap 5 : Mengidentifikasi berbagai Skenario Ancaman

Memperjelas ancaman yang terjadi pada setiap *area of concern*. Hasil dari tahap lima adalah sebagai berikut:

1) Pelaku ancaman

Pada 52 *area of concern* tercatat bahwa kategori internal Perpustakaan X tercatat ada 14 pelaku, kategori internal Universitas X ada 13 pelaku dan sisanya ada 2 pelaku dari kategori eksternal.

Tabel 3 Pelaku Ancaman

Aset Informasi	Pelaku		
	Internal		Eksternal
	Perpustakaan X	Universitas X	
Data kebutuhan koleksi baru	a. Ka UPT Perpustakaan b. Kasub unit layanan administrasi c. Staf Unit Layanan administrasi d. Staf Perawatan dan Pemeliharaan	a. Dosen b. Mahasiswa c. Staf pemeliharaan jaringan (UPT Multimedia) d. Tidak diketahui	Tidak diketahui

Informasi proses pembelian koleksi baru	a. Staf unit layanan administrasi b. Tidak diketahui	a. Warek I b. Dewan Audit c. Tidak diketahui	Tidak diketahui
Data koleksi baru	a. Kasub unit pengolahan b. Staf unit pengolahan c. Staf Perawatan dan Pemeliharaan	UPT Multimedia	Pihak pengembang SIPRUS
Dokumen elektronik koleksi X-ana	a. Staf unit pengolahan b. Tidak Diketahui	a. Tidak diketahui b. Pembuat dolumen X-ana c. Tidak diketahui	Tidak diketahui
Sistem pengelolaan infrastruktur dan penanggulangan bencana	a. Ka UPT Perpustakaan b. Staf perpustakaan c. Staf Perawatan dan Pemeliharaan d. Tidak diketahui e. Administrator	a. Tidak diketahui b. Ka UPT Puskom c. Staf UPT Puskom d. Staf UPT Multimdia e. Pengguna jaringan f. Pengguna komputer	Pihak pengembang SIPRUS
Data anggota	a. Staf perpustakaan b. Saf Layanan Sirkulasi	a. BAA b. Anggota	Pihak pengembang SIPRUS
Data koleksi perpustakaan	a. Ka UPT Perpustakaan b. Kasub unit layanan administrasi c. Staf Layanan Sirkulasi	Anggota	
Modul literasi informasi	a. Ka UPT Perpustakaan b. Kasub Unit Layanan Referens		
Koleksi multimedia (audiovisual)	a. Ka UPT Perpustakaan b. Kasub unit layanan administrasi c. Staf Layanan Multimedia d. Staf Perawatan dan pemeliharaan		
Koleksi *e-journal* dan *database* online	a. Staf Layanan Referens/Multimedia b. Staf perpustakaan	a. Dosen b. Mahasiswa	

Dengan diketahuinya para pelaku ancaman, maka dapat diidentifikasi pula bagaimana pelaku melakukan ancaman dan alasan mengapa pelaku melakukan ancaman. Sebagai contoh dapat dilihat pada Tabel 5 di bawah ini.

Tabel 5 Ancaman pada A*rea of Concern*

Area concern	**Ancaman**	
Usulan kebutuhan koleksi baru yang disampaikan kepada perpustakaan tidak mempunyai data bibliografi yang jelas	***Actor***	Dosen Mahasiswa
	Means	Mengusulkan kebutuhan koleksi baru yang tidak lengkap data bibliografinya sehingga perpustakaan bisa salah mendata koleksi yang dimaksud oleh pengusul
	Motives	Ketidaksengajaan karena tidak mengetahui data bibliografi yang lengkap
	Outcome	*Destruction* *Modification*
	Security requirements	Memastikan usulan semua pihak disertai dengan data bibliografi yang lengkap
	Probability	Sedang

2) Akibat ancaman

Untuk akibat (*outcome*) dari skenario ancaman yang dapat menyebabkan aset informasi menjadi terbuka (*disclosure*) terdapat pada 7 *area of concern*, menyebabkan rusak (*destruction*) terdapat pada 27 *area of concern*, menyebabkan perubahan (*modification*) ada pada 6 *area of concern*, dan yang dapat menyebabkan layanan terganggu (*interruption*) ada pada 34 *area of concern.*

3) Peluang ancaman

Untuk kemungkinan atau peluang terjadinya ancaman dicatat pada probabilitas (*probability*). Pada *probability* terdapat tiga pilihan nilai, yaitu : tinggi-sedang-rendah. Peluang yang paling sedikit adalah kategori sedang sebanyak 16 probabilitas, kategori tinggi sebanyak 17 probabilitas, dan kategori rendah sebanyak 19 probabilitas.

Tahap 6 : Mengidentifikasi Risiko

Hasil dari analisis terhadap risiko diperoleh 62 konsekuensi dari 52 *area of concern* jika skenario ancaman terjadi. Konsekuensi yang terbanyak ada pada dokumen elektronik koleksi X-ana, yaitu dari 6 *area of concern* menghasilkan 10 konsekuensi.

Tahap 7 : Menganalisis Risiko

Tahap 7 ini melakukan analisis terhadap total risiko yang merupakan hasil tahap 4, 5, dan 6. Hal ini dilakukan dengan mengkuantifikasikan kriteria pengukuran risiko dari tahap 1. Hasil kuantifikasi ini disebut skor risiko relatif yang diperoleh dengan cara menghitung skor untuk setiap area dampak dengan mengalikan nilai area dampak dengan nilai prioritas area dampak yang diperoleh dari urutan prioritas yang telah dibuat pada tahap 1. Kemudian nilai dampak dikuantitatifkan sebagai berikut : rendah (nilai 1), sedang (nilai 2), dan tinggi (nilai 3). Jumlah hasil perkalian tersebut di atas dan hasilnya adalah skor risiko relatif.

Tabel 6 Cara Menghitung Skor terhadap Area Dampak

Area dampak	Prioritas	Nilai Prioritas	Nilai dampak		
			Rendah (1)	Sedang (2)	Tinggi (3)
Reputasi dan Kepercayaan Pengguna	1	6	6	12	18
Keamanan	2	5	5	10	15
Produktivitas	3	4	4	8	12
Hukum dan Peraturan	4	3	3	6	9
Keuangan atau Biaya operasional	5	2	2	4	6
Kesehatan dan Keselamatan	6	1	1	2	3

Hasil analisis risiko yang dilakukan pada tahap 7 adalah: skor risiko relatif tertinggi adalah 53 terdapat pada aset informasi dokumen elektronik koleksi X-ana sedangkan sedangkan yang terendah skor risiko relatifnya adalah 29 ada pada aset informasi proses pembelian koleksi baru.

Tabel 7 Skor Risiko Relatif

Aset Informasi	Skor risiko relatif	
	Terendah	Tertinggi
Data kebutuhan koleksi baru	30	39
Informasi proses pembelian koleksi baru	29	39
Data koleksi baru	37	46
Dokumen elektronik koleksi X-ana	38	53
Sistem pengelolaan infrastruktur dan penanggulangan bencana	37	49
Data anggota	34	51
Data koleksi perpustakaan	38	47
Modul literasi informasi	33	33
Koleksi multimedia (audiovisual)	33	43
Koleksi *e-journal* dan *database* online	33	43

Tahap 8 : Memilih Pendekatan Mitigasi

Pendekatan mitigasi merupakan cara bagaimana Perpustakaan X akan memutuskan untuk mengatasi risikonya. OCTAVE Allegro memberikan pendekatan mitigasi yang dapat dipilih, yaitu : menerima (*accept*), mitigasi atau mengurangi (*mitigate*), dan menunda (*defer*). Untuk memulai mitigasi, pertama mengurutkan masing-masing risiko skor relatifnya. Kemudian dibuat pengkategorian untuk memudahkan melakukan pendekatan mitigasi setiap risiko. Pengelompokan berdasarkan skor risiko relatif hasil analisis risiko tahap 7 dan probabilitas terjadinya ancaman hasil tahap 5.

Tabel 8 Matriks Risiko Relatif dengan Probabilitas Ancaman

Probabilitas	Skor risiko relatif		
	(46 – 53)	(38 – 45)	(29 – 37)
Tinggi	Kategori 1	Kategori 2	Kategori 3
Sedang	Kategori 2	Kategori 3	Kategori 4
Rendah	Kategori 3	Kategori 4	Kategori 4

Masing-masing kategori tersebut di atas dapat menggambarkan tingkat kerawanan informasi, yaitu sebagai berikut:

1. Kategori 1 merupakan tingkat yang paling rawan informasinya.
2. Kategori 2 merupakan tingkat yang rawan informasinya.
3. Kategori 3 merupakan tingkat yang cukup rawan informasinya.
4. Kategori 4 merupakan tingkat yang tidak rawan informasinya.

1) Tingkat kerawanan informasi

Dengan melihat probabilitas ancaman dan nilai skor relatif pada setiap *area of concern* yang diwakili oleh nomor urutannya dimasukan ke dalam kategori berdasarkan ketentuan masing-masing kategori. Dengan berpedoman pada matriks risiko relatif, maka hasil dari tahap ini adalah sebagai berikut:

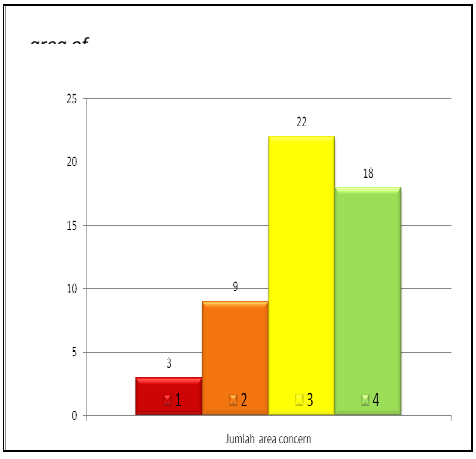
a). Kategori 1 terdapat 3 *area of concern*. Terdapat pada aset informasi Data koleksi baru, Dokumen elektronik X-ana, dan Sistem pengelolaan infrastruktur dan penanggulangan bencana.

b). Kategori 2 dengan probabilitas tinggi dan nilai sedang ada 6 *area of concern*. Kategori 2 dengan probabilitas sedang dan nilai tinggi ada 3 *area of concern*.

c). Kategori 3 dengan probabilitas tinggi dan nilai rendah ada 8 *area of concern*. Kategori 3 dengan probabilitas sedang dan nilai sedang ada 8 *area of concern*. Kategori 3 dengan probabilitas rendah dan nilai tinggi ada 6 *area of concern*. Terdapat pada semua aset informasi kecuali Modul literasi informasi.

d). Kategori 4 dengan probabilitas sedang dan nilai rendah ada 5 *area of concern*. Kategori 4 dengan probabilitas rendah dan nilai sedang ada 6 *area of concern*. Kategori 4 dengan probabilitas rendah dan nilai rendah ada 7 *area of concern*.

Agar lebih jelas pengelompokan kategori yang memberikan gambaran tingkat kerawanan informasi di Perpustakaan X dapat dilihat pada Gambar 4 di bawah ini.



Gambar 4 *Area of Concern* Berdasarkan Kategori Kerawanan

Gambar 4 tersebut di atas menunjukan bahwa *area of concern* yang ada di Perpustakaan X yang masuk tingkat 1 atau kategori sangat rawan sebesar 5.77%. Pada tingkat 2 atau kategori rawan sebesar 17.31%. Tingkat 3 atau kategori cukup rawan sebesar 42.31%, dan yang terakhir pada tingkat 4 atau tidak rawan sebesar 34.61%. Dengan demikian maka dapat disimpulkan bahwa Perpustakaan X berada pada tingkat kerawanan informasi cukup rawan karena *area of concern* yang terbanyak berada pada kategori 3 atau cukup rawan.

2) Pendekatan mitigasi

Selanjutnya menetapkan pendekatan mitigasi untuk setiap risiko. Berdasarkan analisis di atas, maka ditetapkan status mitigasi untuk Perpustakaan X, yaitu:

Tabel 9 Pendekatan dan Pengurangan Risiko

Kategori	Tindakan	Jumlah *area of concern*
1	Mitigasi (mitigate)	21
2	*Transfer*/Mitigasi	16
3	Menunda/Mitigasi	19
4	Menerima/Menunda	3

3) Strategi mitigasi

Hasil pengurangan risiko adalah sebagai berikut: *mitigate* yang dilakukan pada *container* prosedur sebanyak 12 tindakan, pada *container* data sebanyak 3 tindakan, pada *container hardware* sebanyak 2 tindakan, dan pada orang (*people*) sebanyak 4 tindakan. Pengurangan risiko dengan *transfer* dilakukan pada *container* prosedur sebanyak 7 tindakan, pada *container* data sebanyak 3 tindakan, pada *hardware* sebanyak 3 tindakan, pada *people* sebanyak 4 tindakan, dan pada *software* dan aplikasi hanya 1 tindakan. Kemudian tindakan *defer* dilakukan pada prosedur sebanyak 6 tindakan, pada data sebanyak 2 tindakan, pada *people* terdapat 3 tindakan, dan pada *software* hanya 1 tindakan. Tindakan *accept* masing-masing 1 tindakan untuk *container* prosedur, data dan *people*. Pengurangan risiko dilakukan sesuai masing-masing *area of concern* yang disebut kontrol. Berbagai kontrol inilah yang dijadikan rekomendasi kepada pihak manajemen Perpustakaan X dalam penilaian risiko ini untuk mengurangi kerawanan informasi yang ada.

Kesimpulan

Penilaian risiko pada dasarnya merupakan proses identifikasi terhadap aset informasi, ancaman, dan kerawanan. Dengan menggunakan metode OCTAVE Allegro maka hasil penilaian risiko dapat dilakukan.

Perpustakaan X memiliki 10 aset yang dianggap kritis. Tiga aset dimiliki oleh Ka UPT Perpustakaan. Satu aset dimiliki Kasub unit layanan administrasi yaitu Data koleksi baru. Satu aset milik Kasub unit pengolahan. Dua aset milik Kasub unit layanan sirkulasi. Sisanya tiga aset milik oleh Kasub Unit Referens. Pemilik aset informasi disini merupakan para pengelola yang bertanggungjawab terhadap kelangsungan dan keamanan aset informasi di Perpustakaan X. Pada 10 aset informasi yang ada pada Perpustakaan X terdokumentasi ada 10 aset yang memiliki integritas. Sembilan aset informasi kritis memiliki kerahasiaan. Tujuh aset yang memiliki ketersediaan. Serta ada dua aset yang memiliki karakteristik kepemilikan (*possession)*. Lima aset informasi dinyatakan integritas sebagai syarat keamanan terpenting pada aset informasi. Sedangkan sisanya lima aset dinyatakan ketersediaan sebagai persyaratan keamanan yang paling penting.

Area of concern merupakan salah satu ancaman bagi aset informasi dimana terdapat sebanyak 52 *area of concern* yang berasal dari 10 aset informasi. Pelaku ancaman terhadap aset informasi di Perpustakaan X dibagi dalam 3 kategori. Kategori internal Perpustakaan X tercatat ada 14 pelaku, kategori internal

Usakti ada 13 pelaku dan sisanya ada 2 pelaku dari kategori eksternal. Skenario ancaman yang dapat menyebabkan aset informasi menjadi terbuka (*disclosure*) terdapat pada 7 *area of concern*, menyebabkan rusak (*destruction*) terdapat pada 27 *area of concern*, menyebabkan perubahan (*modification*) ada pada 6 *area of concern*, dan yang dapat menyebabkan layanan terganggu (*interruption*) ada pada 34 *area of concern.* Peluang yang paling sedikit adalah kategori sedang yaitu sebanyak 16 probabilitas, kategori tinggi sebanyak 17 probabilitas, dan kategori rendah sebanyak 19 probabilitas.

Ada 62 konsekuensi dari 52 *area of concern* jika skenario ancaman terjadi. Konsekuensi yang terbanyak ada pada dokumen elektronik koleksi X-ana, yaitu dari 6 area *of concern* menghasilkan 10 konsekuensi,

Gambaran tingkat kerawanan informasi berdasarkan matriks nilai risiko relatif berada pada kategori 3 atau tingkat cukup.

Untuk mengatasi berbagai kerawanan informasi yang ada, Perpustakaan X perlu menyesuaikan pengurangan risiko yang dilakukan pada masing-masing *area of concern* yang disebut kontrol atau kendali risiko. Dari hasil penilaian risiko ini, yang dapat dilakukan adalah mengurangi atau menghilangkan risiko (*mitigate*) sebanyak 21 *area of concern*, memindahkan risiko (*transfer*) atau mitigate sebanyak 16 *area of concern*, menunda risiko (*defer*) sebanyak 12 *area of concern*, dan menerima risiko (*accept*) atau menunda sebanyak 3 *area of concern*.

Daftar Pustaka

Brunschwiler, Cyrill (2013) Lean Risk Assessment based on OCTAVE Allegro https://blog.csnc.ch/ 2013/04 /lean-risk-assessment-based-on-octave-allegro/ [Diakses 16 September 2015**]**

Caralli, RA, JF, Steven, R, Young, WR, Wilson (2007) *Introducing OCTAVE Allegro: improving the information security risk assessment process.* Software Engineering Institute Carnegie Mellon University **CMU/SEI Report Number:** CMU/SEI-2007-TR-012 http://resources.sei.cmu.edu/library/asset-view.cfm? assetid=8419. [Diakses 13 Juni 2011].

Keating, Corland G (2014) Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study [Dissertation]. Graduate School of Computer and Information Sciences Nova Southeastern University. http://media.proquest.com/media/pq/classic/doc/3238417401/fmt/ai/rep/NPDF? s=aFRBvZcffJfVljMUcMt%2B2Rw5erA%3D [Diakses 16 September 2015].

Maček, Davor, I.M., Nikola Ivković (2011) *Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods.* http://www.ceciis.foi.hr/app/index.php/ceciis/2011/paper/viewFile/478/259 [Diakses 16 September 2015]

Taylor, AG, Joudrey, DN (2009) *The Organization of Information.* Westport, Connecticut (US): Libraries Unlimited

Whitman, ME, Mattord, HJ (2012) *Principes of Information Security.* Boston (US): Course Technology, Thomson