JURNAL FASILKOM
(FAKULTAS ILMU KOMPUTER)
Vol. 8 Nomor 1 (2019) 289 –298 ISSN : 2089-3353

IDENTIFIKASI RISIKO ASET INFORMASI PADA SISTEM INFORMASI AKADEMIK

Risnal Diansyah1) , Ikko Claudya Armae 2), Melly Novalia3), Nesdi E. Rozanda4)
[1,2)] Sistem Informasi dan Universitas Muhammadiyah Riau
[3)] Pendidikan Informatika dan Universitas Muhammadiyah Riau
Jl. KH. Ahmad Dahlan No. 88, Sukajadi, Pekanbaru, Telp : (0761) – 35008, Fax : (0761) – 20497
Email : risnal@umri.ac.id, ikkoclaudyaarmae@student.umri.ac.id, mellynovalia@umri.ac.id

ABSTRAK

Pengelolaan akademik di Universitas Muhammadiyah Riau (UMRI) didukung oleh penerapan Teknologi Informasi (TI) berupa Sistem Informasi akademik. Aktivitas yang dilakukan melalui sistem informasi akademik diantaranya proses registrasi perkuliahan mahasiswa, proses hasil studi mahasiswa, data master dosen & mahasiswa, penjadwalan perkuliahan, absensi perkuliahan, dan monitoring catur dharma dosen. Penerapan sistem informasi akademik dapat menimbulkan risiko apabila UMRI gagal dalam menilai sumber ancaman risiko. Manajemen risiko merupakan suatu upaya dari perencanaan, pengorganisasian, kepemimpinan, pengendalian sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian dan ketidakpastian terhadap biaya serta konsekuensinya. Pada PP No. 20 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah, pada bagian ketiga Pasal 13 diatur bahwa setiap pimpinan instansi pemerintah wajib melakukan penilaian risiko. Penilaian risiko yang dimaksud adalah tentang penilaian risiko terhadap keamanan sistem informasi. Dengan demikian, Manajemen risiko terhadap sistem informasi sudah seharusnya dilakukan oleh organisasi yang memanfaatkan Teknologi Informasi dalam mendukung aktivitasnya sebagaimana yang ada di UMRI. Metode Octave Allegro merupakan merupakan metodologi untuk mengidentifikasi risiko pada sistem informasi terkait dengan keamanan sistem Informasi. Octave mendefinisikan komponen-komponen penting secara komprehensif, sistematis, berbasis konteks evaluasi risiko keamanan sistem informasi. Metode Octave Allegro terdiri dari delapan tahapan. Hasil akhir dari penelitian ini adalah 8 aset krusial dengan penilaian 1 aset berisiko rendah, 5 aset berisiko sedang, dan 2 aset berisiko tinggi.

Kata Kunci : Aset, Identifikasi aset, *Sistem Informasi Akademik, Risiko, Manajemen Risiko*

ABSTRACT

Academic management at Muhammadiyah University of Riau (UMRI) is supported by the application of Information Technology (IT) in the form of academic information system. Activities undertaken through the academic information system include the registration process of students' learning, the process of study results, lecturer & student master data, learning schedule, attendance, and lecturer Catur Dharma monitoring. The implementation of academic information systems may be at a risk if UMRI fails to assess the source of the risk.. Risk management is an effort of planning, organizing, leadership, resources controlling and activities to minimize the impact of loss and uncertainty on costs and consequences. In Government Regulation number 20 of 2008 about Government Internal Control System, in the third part of Article 13, it is stipulated that every leader of government agencies must perform risk assessment. The risk assessment is about risk assessment of information system security. Thus, risk management of information systems should be done by organizations that utilize Information Technology in supporting their activities as in UMRI.. Octave Allegro method is a methodology for identifying risks towards information systems related to information systems security. Octave defines the critical components in a comprehensive, systematic, context-based evaluation of information systems security risks. The Octave Allegro method consists of eight stages.

The final result of this study is in the form of a risk assessment table and mitigation of risks to information assets. There are 8 (eight) crucial assets with a level of risk assessment of as low as 1 (one), moderate as much as 5 (five) and high as much as 2 (two).

Keyword : Asset, Asset identification, Academic Information System, Risk, Risk Management

1.1 Latar Belakang

Teknologi informasi merupakan salah satu faktor pendukung meningkatnya produktivitas proses bisnis dari suatu organisasi pada era globalisasi yang semakin berkembang pesat. Penerapan teknologi informasi tentunya harus diimbangi dengan pengelolaan yang memadai. Sama halnya dengan penyedia layanan pendidikan yang memerlukan informasi sebagai pondasi keberhasilan kinerjanya. Salah satu penerapan teknologi informasi dalam bidang akademik adalah sistem informasi akademik. Menurut Rilyani (2015), sistem informasi akademik merupakan salah satu sistem terintegrasi yang menjadi media penghubung antara citivitas akademik. Dengan demikian, sistem informasi dapat mempermudah pekerjaan dan mempercepat proses pekerjaan yang berkaitan dengan kegiatan akademik di lembaga pendidikan.

Universitas Muhammadiyah Riau (UMRI) merupakan salah satu lembaga pendidikan swasta yang berada di Provinsi Riau. Kegiatan akademik di UMRI sudah didukung oleh teknologi informasi berupa Sistem Informasi Akademik Universitas Muhammadiyah Riau. Sistem Informasi Akademik di UMRI digunakan sejak tahun 2010. Sistem Informasi Akademik didukung oleh berbagai fitur yang memungkinkan Civitas Akademik di UMRI dapat berinteraksi melalui sistem yang sudah terintegrasi. Aktivitas yang biasanya dilakukan melalui Sistem Informasi Akademik antara lain, registrasi akademik, penjadwalan perkuliahan, hasil akademik, master data dosen dan mahasiswa, dan lain-lain. Peningkatan penggunakaan Teknologi Informasi di bidang akademik khususnya penggunaan sistem informasi di UMRI, juga sejalan dengan meningkatnya risiko Teknologi Informasi yang harus dihadapi UMRI. Hal ini terjadi karena selain efek positif yang muncul akibat berkembangnya sistem informasi maka permasalahan keamanan dan pengelolaan sumber daya TI juga terjadi. Masalah keamanan yang dimaksud pada pernyataan ini berkaitan dengan risiko pada Teknologi Informasi.

Pada penelitian ini, dilakukan tahapan identifikasi resiko dimana, pada tahapan awal akan dilakukan identifikasi terhadap aset-aset informasi pada penerapan sistem informasi akademik di Universitas Muhammadiyah Riau.

2. Methode yang digunakan

Dalam melakukan identifikasi aset informasi dilakukan dengan tiga tahapan menggunakan worksheet yang dikembangkan oleh octave allegro. Berikut ini adalah tahapan identifikasi aset yang dilakukan.

2.1 Mengembangkan Profil Asset Informasi

Penilaian risiko yang dilakukan berfokus pada penilaian asset informasi Sistem Informasi Akademik. Dilangkah ini dimulai dengan mendefinisikan asset informasi Sistem Informasi Akademik, berupa nama, deskripsi pengguna, dan proses inti dalam menjalankan aset tersebut. Hal ini membantu TIPD UMRI untuk mengidentifikasi semua asset informasi rentan untuk diungkap, modifikasi, hilang/rusak, dan interupsi. Profil dibuat untuk setiap asset informasi.

2.2 Mengidentifikasi aset krusial

Untuk menentukan asset informasi kritikal pada Sistem Informasi Akademik, dapat dilihat dari proses sistem, aktivitas apa saja yang terkait dengan sistem. Sistem Informasi Akademik digunakan oleh UMRI untuk kegiatan pengolahan data mahasiswa dan pegawai/dosen yaitu mengolah profil lengkap mahasiswa dan dosen, dan data keuangan mahasiswa. Sistem Informasi memiliki beberapa kegunaan dengan terbagi menjadi beberapa modul yaitu modul pegawai dan dosen serta modul mahasiswa. Adapun bentuk tabel untuk menentukan asset informasi kritikal yang berisikan modul, pengguna dan proses inti. Modul maksudnya bagian sistem informasi yang digunakan dan didalam modul terdapat menu-menu untuk aktivitas sistem. Pengguna maksudnya adalah pemilik maupun pihak yang mengoperasikan modul tersebut. Dan proses inti maksudnya adalah aktivitas yang dilakukan pada sistem informasi yang digunakan. Sebelum melakukan penentuan asset informasi yang paling kritikal, maka digunakan worksheet *critical asset worksheet* sebagai berikut :

Tabel 1.1 *Critical asset (Nama menu)*

Critical Asset	(Nama menu)
Rationalfor Selection	
Deskription	
Owner	

Security Requirements	*Confidentiality*	
	Integrity	
	Availability	
ImportantSecurity Requirement		

Pada tabel 1.1 *Critical asset* adalah menentukan menu yang akan didokumentasikan pada kolom (1). Langkah selanjutnya*Rationale for selection*digunakan untuk dokumentasikan alasan untuk memilih asset informasi kritis pada kolom (2) pada *Critical Information Asset Profil*. Lalu mengisi sebuah deskripsi mengenai asset informasi kritis dalam kolom (3) dari *Critical Information Asset Profil*. Definisikan ruang lingkup dari *Information Asset* dan bahwa akan digunakan definisi yang telah disepakati dan umum. Kemudian identifikasi dan didokumentasikan pemilik dari asset informasi kritis (mengacu pada definisi yang disediakan untuk menentukan mana sebagai pemilik). Informasi ini diisi pada kolom (4) Profil Aset Informasi Kritis. Selanjutnya mengisi kebutuhan kemanan untuk *Confidentiality* maksudnya kerahasiaan informasi dari asset tersebut, *Integrity* maksudnya kebenaran dan keakuratan dari informasi pada asset terkait dan *Availability* maksudnya adalah ketersediaan informasi pada asset informasi terkait pada kolom (5) pada *Critical Information Asset Worksheet*. Dimulai dengan menandai kebutuhan yang dapat diaplikasikan pada asset informasi dan diteruskan dengan mengisi informasi yang melengkapi pernyataan kebutuhan keamanan. pada sebelah kanan dari pernyataan ini dapat ditambahkan kebutuhan atau dapat dibuatkan kebutuhan yang lebih spesifik. Lalu langkah selanjutnya mengidentifikasi kebutuhan keamanan yang paling penting untuk asset informasi dengan memilih salah satu kebutuhan keamanan dalam kolom (6) pada *Critical Information Asset Worksheet*. Informasi ini digunakan ketika ditentukannya dampak potensial dari risiko.

2.3 Mengidentifikasi Container Asset Informasi

Terdapat 3 poin yang sangat penting tentang keamanan dan konsep dari *container asset* informasi yaitu *technical, people dan physical*. *Container* merupakan tempat dimana asset informasi disimpan, dikirim, atau diproses sehingga dapat menjadi poin dari kerentanan dan ancaman yang memposisikan asset informasi pada risiko, dan sebaliknya *container*, dapat menjadi tempat dimana control dapat diimplementasikan.

Container secara khusus diidentifikasi dari beberapa tipe dari asset teknologi informasi seperti perangkat keras, perangkat lunak atau sistem. Yang pertama dilakukan yaitu menentukan asset informasi pada *container asset technical* yang meliputi asset teknologi (perangkat lunak, sistem aplikasi, server, jaringan atau perangkat keras) ,*container physical* juga bisa berupa objek fisik seperti kertas dan *container people* berupa kepemilikan seperti siapa pengguna asset informasi tersebut. Berikut adalah bentuk dari tabel container asset technical, people dan physical. Untuk melakukan identifikasi container aset maka digunakan worsheet berikut ini:

Tabel 1.2 Container asset (nama menu)

Menu Data Pegawai dan Dosen	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
External	**Owner(s)**
Container Description	-

Pada tabel 1.2 *container asset technical* pada kolom (1) digunakan untuk mengisi nama menu,*information asset risk environment map (technical)* pada kolom (2) untuk menyatakan pemetaan lingkungan risiko asset informasi meliputi perangkat lunak, perangkat keras, server, sistem aplikasi, *Internal* pada kolom (3)untuk menyatakan pihak organisasi yang menggunakannya. *Container description* untuk deskripsi mengenai asset informasi yang disimpan, dikirim dan diproses terdapat pada kolom (4). Owners untuk menyatakan siapa

pemilik atau pengguna sistem tersebut terdapat pada kolom (5). Dan pada kolom (6) untuk menyatakan ada tau tidak pihak luar yang terkait dalam aktivitas pada sistem informasi terkait.

Container asset people untuk menyatakan siapa pemilik atau pengguna dari sistem informasi terkait, serta yang membawa dan menyimpan asset informasi. Seperti pada *container description* nya berisikan pengguna terkait sistem informasi yang digunakan, sedangkan *owners* nya adalah nama dari asset informasi yang digunakan.

Container asset physical digunakan untuk menyatakan folder berkas tempat dimana disimpan dalam bentuk fisik, kertas misalnya. Seperti pada tabel 1.4 *container asset physical* menu data pegawai

untuk *container description* nya berisikan sk/slip gaji, sedangkan *owners* nya adalah pegawai dan dosen terkait.

2.4 Mengidentifikasi Area of Concern

Pada langkah ini, yang perlu dilakukan adalah pengembangan profil risiko asset informasi. Karena risiko merupakan kombinasi ancaman (kondisi) dan dampak yang dihasilkan dari ancaman jika ditindaklanjut (akibatnya). Berikut *critical asset worksheet* yang digunakan:

Tabel 1.3 *Area of Concern* (nama menu)

No	*Area of Concern* (nama menu)

Pada tabel 1.3 *Area of concern* adalah pernyataan yang menjelaskan kondisi atau situasi sebenarnya di dunia nyata yang dapat memengaruhi asset informasi di dalam organisasi atau perusahaan.

2.5 Mengidentifikasi Skenario Ancaman

Langkah sebelumnya yaitu langkah 4 (empat) telah didokumentasikan *area of concern*. Pada tahap ini *area of concern* dikembangkan ke dalam scenario ancaman yang menjelaskan detail atribut dari sebuah risiko. Untuk mengembangkan *area of concern* menjadi scenario ancaman. Berikut adalah tabel *Threat Properties* yang digunakan :

Tabel 1.4 *Threat Properties*

.	***Area of Concern***	***Threat of Properties***	
		1. Actor	
		2. Means	
		3. Motives	
		4. Outcome	
		5. Security Requirements	

Tabel 1.4 *Threat Properties* pada kolom (1) untuk mengisi pernyataan yang menjelaskan kondisi atau situasi sebenarnya di dunia nyata yang dapat memengaruhi asset informasi di dalam organisasi atau perusahaan. Pada kolom (2) untuk mengisi skenario ancaman yang terdapat beberapa atribut seperti aset : sesuatu yang memiliki nilai bagi perusahaan. Akses/alat : bagaimana asset diakses oleh actor (akses teknik, akses fisik), akses hanya berlaku kepada actor manusia. Aktor : siapa saja atau apa saja yang dapat melanggar persyaratan keamanan (kerahasiaan, integritas, ketersediaan) di suatu asset. Motif : tujuan dari actor (sengaja atau tidak sengaja). Hasil : hasil (pengungkapan, modifikasi, kerusakan, kerugian, gangguan) apa dampaknya terhadap asset informasi.

2.6 Mengidentifikasi Risiko

Dengan mengidentifikasikan bagaimana sistem informasi terkena dampak dari risiko, persamaan risiko dapat digambarkan sebagai berikut : Ancaman (kondisi) + dampak (konsekuensi) = risiko, |langkah 4 dan 5| + |langkah 6| = risiko, maksudnya adalah langkah 4 merupakan pemetaan lingkungan risiko asset informasi + langkah 5 adalah output dari langkah 4 yang merupakan hasil pengembangan scenario ancaman dari area of concern + langkah 6 adalah mengidentifikasi risiko merupakan konsekuensi dari scenario ancaman (kondisi) = risiko. Berikut tabel Nilai *Priority Impact Area* untuk mengukur risiko aset informasi:

Tabel 1.5 Nilai *Priority Impact Area*

Impact Areas	***Priority***	***Low(1)***	***Medium(2)***	***High(3)***
Produktivitas	1	5	10	15
Reputasi dan Kepercayaan	2	4	8	12
Financial	3	3	6	9
Denda dan Hukuman	4	2	4	8
Keamanan dan Kehidupan	5	1	2	3

Pada tabel 1.5 *impact area* terdapat kolom penilaian priority untuk mengukur criteria semua aset informasi yang penting yang terdapat pada sistem informasi akademik.

2.7 Menganalisa Risiko

Pada langkah 7 (tujuh), diberikannya nilai kualitatif kepada jangkauan sejauh mana Sistem Informasi Akademik diperngaruhi oleh ancaman dengan cara menghitung nilai risiko untuk tiap risiko terhadap setiap asset informasi.

Penilaian ini digunakan untuk menentukan risiko mana yang membutuhkan langkah mitigasi secepatnya dan untuk memprioritaskan tindakan mitigasi secepatnya dan untuk memprioritaskan tindakan mitigasi pada langkah 8 (delapan). Pada penilaian risiko terstruktur, akan dilakukan aktivitas yang memberikan langkah sistematis untuk menganalisa bagaimana Sistem Informasi Akademik terpengaruh oleh suatu risiko. Pada aktivitas ini akan dihasilkan nilai risiko relative. Nilai risiko relative dihasilkan dari menghitung jangkauan dari dampak yang dihasilkan suatu risiko terhadap perusahaan terhadap nilai relative kepentingan pada macam-macam *Impact Area*. Berikut adalah tabel *Information Asset Risk* :

Tabel 1.6 *Information Asset Risk* (nama menu)

Area of Concern	***Risk***			
	Consequences			
	Severity	***Impact Area***	***Value***	***Score***
		Produktivitas		
		Reputasi dan Kepercayaan		
		Finansial		
		Denda dan Hukuman		
		Keamanan dan Kehidupan		
		Relative Risk Score		

Pada tabel *Information Asset Risk* terdapat kolom (1) *area of concern* untuk mengisi pernyataan yang menjelaskan kondisi atau situasi sebenarnya. kolom (2) *Consequences* untuk mengisi apa akbibatnya jika terjadi. Kolom (3*) impact area* untuk menentukan urutan impact area. Kolom (4) *value* untuk mengisi nilai yang tertinggi atau terendah. Kolom (5) *score* untuk memberikan point angka, dilihat dari nilai *priority impact area*. Kolom (6) *relative risk score* untuk mengisi total dari score yang telah diberikan.

2.8 Memilih Pendekatan Mitigasi

Pada langkah 8 (delapan) ini, ditentukan risiko yang dimitigasi, disediakan tabel *risk score* untuk menentukan risiko dimitigasi, dibiarkan atau diterima oleh perusahaan.

Tabel 1.7 *Risk Score Information Asset*

RISK SCORE		
30 TO 45	**16 TO 29**	**0 TO 15**
POOL 1 (High)	POOL 2 (Moderate)	POOL 4 (Low)

Pada langkah 8 kegiatan pertama yang dilakukan adalah memilah masing-masing risiko yang telah identifikasi dengan skor risikonya. Mengkategorikan risiko secara teratur akan membantu mulai membuat keputusan tentang status mitigasi. Satu metode sederhana adalah memulai dengan menyortir risiko dalam urutan dari tertinggi ke terendah. Kemudian pisahkan risiko menjadi tiga kolam dengan jumlah risiko yang sama. Risiko dengan skor tertinggi harus di yang pertama (Pool 1), risiko dengan rentang skor tertinggi berikutnya di kedua (Pool 2), dan skor terendah dalam keempat (Pool 4).

Tabel 1.8 *Mitigation Approach Information Asset*

Pool	***Mitigation Approach***
Pool 1 (31 - 45)	*Mitigate*
Pool 2 (16 - 30)	*Mitigate or Defer*
Pool 4 (0 – 15)	*Accept*

Pendekatan mitigasi pool 1 adalah *mitigate* maksudnya adalah tindakan yang diambil jika score relative risiko sangat tinggi, sehingga perlakuan risiko langsung dipimpin oleh Direktur terkait. Pool 2 adalah *mitigate/defer* maksudnya adalah tindakan yang diambil jika score relative risiko cukup tinggi, sehingga perlakuan risiko setingkat dan perlu perhatian Direktur terkait atau cukup menggunakan SOP yang ada, atau SOP baru, atau perlu perbaikan SOP guna memastikan keefektifannya sebagai *risk control*. Pool 4 adalah *accept* maksudnya adalah jika score relative risiko rendah sehingga tidak perlu perlakuan risiko tertentu, cukup dimonitor saja.

Tabel 1.9 *Risk Mitigation* Menu Data Pegawai

Risk Mitigation	
Area of Concern	
Action	
Container	

Pada tabel *risk mitigation* kolom (1) *area of concern* untuk mengisi pernyataan yang menjelaskan kondisi atau situasi sebenarnya di dunia nyata yang dapat memengaruhi asset informasi di dalam organisasi. Kolom (2) *action* untuk mengisi tindakan yang diberikan untuk mengatasi risiko pada aset informasi pada organiasi. Kolom (3) *container* untuk pengontrolan kerentanan dan ancaman dari aset informasi.

2.9 Tahapan Pengumpulan Data

Metode pengumpulan data dilakukan untuk memperoleh informasi, data utama serta data pendukung lainnya yang dibutuhkan dalam rangka mencapai tujuan penelitian. Pengumpulan data dapat diperoleh dari objek penelitian dengan cara sebagai berikut :

1. Studi Pustaka
   Kegiatan studi pustaka dilakukan dengan cara mempelajari dan meneliti berbagai literatur. Literatur tersebut diperoleh dari perpustakaan yang bersumber dari buku-buku, jurnal ilmiah, situs internet, dan bacaan lainnya yang berkaitan dengan penelitian.
2. Studi Lapangan
   Kegiatan studi lapangan dilakukan dengan cara mengadakan penelitian peninjauan secara langsung maupun tidak langsung. Peninjauan tersebut dilakukan pada Kepala UPT Teknologi Informasi dan Pangkalan Data UMRI, dosen, mahasiswa dan karyawan serta tinjauan dokumen.

3. Hasil dan Pembahasan

Berikut ini adalah hasil dari identifikasi aset yang dilakukan

3.1 Mengembangkan Profil Asset Informasi

Penilaian risiko yang dilakukan berfokus pada penilaian asset informasi Sistem Informasi Akademik. Dilangkah ini dimulai dengan mendefinisikan asset informasi Sistem Informasi Akademik, kemudian di identifikasi *container asset*, dimana asset tersebut disimpan dan siapa pemilik asset tersebut. Hal ini membantu TIPD UMRI untuk mengidentifikasi semua asset informasi rentan untuk diungkap, modifikasi, hilang/rusak, dan interupsi. Profil dibuat untuk setiap asset informasi. Pada tahapan ini dihasilkan 11 aset dari sistem informasi akademik.

3.2 Mengidentifikasi aset krusial

Penentuan asset informasi kritikal mengacu pada proses Sistem Informasi Akademik, asset informasi kritikal adalah asset informasi yang digunakan dalam pemrosesan Sistem Informasi Akademik. Asset informasi yang telah ditentukan sebagai asset informasi kritikal akan dicatat pada *critical asset information worksheet*. Asset informasi yang dipilih setelah mempertimbangkan beberapa pertanyaan yaitu :

1. Asset informasi yang penting bagi UMRI
2. Asset informasi yang digunakan dalam kegiatan operasional sehari-hari
3. Asset informasi yang jika hilang, dapat mengganggu kemampuan UMRI dalam mencapai tujuan dan misi UMRI.

Dari hasil pertimbangan diatas terdapat beberapa asset informasi yang dikategorikan asset informasi penting yaitu : Modul pegawai dan dosen terdapat menu data pegawai, menu absen, menu koreksi absen, menu akademik dan menu penelitian dan publikasi. Modul mahasiswa terdapat menu transkrip nilai, menu rencana studi, menu hasil studi, menu kartu ujian, menu jadwal kuliah, menu data pembayaran.

Dari asset informasi yang telah ditentukan, kemudian ditentukan lagi asset informasi benar-benar kritikal bagi UMRI, yaitu asset informasi yang jika terjadi kerusakan akan berdampak besar bagi UMRI jika terjadi hal-hal berikut :

1. Asset informasi tersebut dimodifikasi tanpa otorisasi
2. Asset informasi tersebut hilang atau rusak
3. Asset informasi tersebut diakses oleh orang yang tidak memiliki izin
4. Asset informasi tersebut kritis bagi sistem informasi akademik dan UMRI

Dari pertanyaan-pertanyaan diatas dan pertimbangan TIPD UMRI, yang menjadi asset-aset penting yang bersifat kritis adalah asset informasi yang terdapat pada modul mahasiswa dan modul pegawai & dosen, karena disinilah proses inti dilakukan. Aset informasi kritikal tersebut adalah : Modul pegawai dan dosen terdapat menu data pegawai, menu absen, menu penelitian dan publikasi dan menu akademik. Modul mahasiswa terdapat menu transkrip nilai, menu rencana studi, menu hasil studi dan menu data pembayaran. Kemudian asset kritis diatas didokumenkan pada *critical asset worksheet*, setelah dilakukan mengisi worksheet kritikal asset maka didapatkan 8 tabel asset informasi yang kritikal yaitu menu data pegawai, menu absen, menu penelitian dan publikasi, menu akademik, menu transkrip nilai, menu rencana studi, menu hasil studi dan menu data pembayaran.

3.3 Mengidentifikasi Kontainer dari Aset Informasi

Terdapat 3 poin yang sangat penting tentang keamanan dan konsep dari *container asset* informasi yaitu *technical, people dan physical*. *Container* merupakan tempat dimana asset informasi disimpan, dikirim, atau diproses sehingga dapat menjadi poin dari kerentanan dan ancaman yang memposisikan asset informasi pada risiko, dan sebaliknya *container*, dapat menjadi tempat dimana control dapat diimplementasikan.

secara khusus diidentifikasi dari beberapa tipe dari asset teknologi informasi seperti perangkat keras, perangkat lunak atau sistem. Yang pertama dilakukan yaitu menentukan asset informasi pada *container asset technical*yang meliputi asset teknologi (perangkat lunak, sistem aplikasi, server, jaringan atau perangkat keras) ,*container physical* juga bisa berupa objek fisik seperti kertas dan *container people* berupa kepemilikan seperti siapa pengguna asset informasi tersebut.

Berdasarkan hasil yang didapatkan setelah melakukan container asset pada 3 aspek yaitu technical, people dan physical, bahwa

yang termasuk *container technical* adalah menu data pegawai, menu absen, menu penelitian dan publikasi, menu akademik, menu transkrip nilai, menu rencana studi, menu hasil studi, dan menu data pembayaran. Yang termasuk *container people* adalah menu data pegawai, menu absen, menu penelitian dan publikasi, menu akademik, menu transkrip nilai, menu rencana studi, menu hasil studi dan menu data pembayaran. Sedangkan yang termasuk *container physical* adalah menu data pegawai, menu penelitian dan publikasi, menu akademik, menu transkrip nilai, menu hasil studi dan menu data pembayaran.

3.4 Mengidentifikasi Area of Concern

Setelah melakukan identifikasi kontainer dari aset informasi, selanjutnya perlu melakukan pengembangan profil risiko asset informasi yaitu membuat pernyataan yang menjelaskan kondisi atau situasi sebenarnya di dunia nyata yang dapat memengaruhi asset informasi di dalam organisasi atau perusahaan. Karena risiko merupakan kombinasi ancaman (kondisi) dan dampak yang dihasilkan dari ancaman jika ditindaklanjut (akibatnya).

3.5 Mengidentifikasi Skenario Ancaman

Pada tahap ini *area of concern* dikembangkan ke dalam scenario ancaman yang menjelaskan detail atribut dari sebuah risiko. Ada beberapa atribut-atribut yang menyusun risiko yaitu aset : yang memiliki nilai bagi perusahaan, akses/alat : bagaimana asset diakses oleh actor (akses teknik, akses fisik), akses hanya berlaku kepada actor manusia, aktor : siapa saja atau apa saja yang dapat melanggar persyaratan keamanan (kerahasiaan, integritas, ketersediaan) di suatu asset, motif : tujuan dari actor (sengaja atau tidak sengaja), hasil : hasil (pengungkapan, modifikasi, kerusakan, kerugian, gangguan) apa dampaknya terhadap asset informasi.

3.6 Mengidentifikasi Risiko

Dengan mengidentifikasikan bagaimana sistem informasi terkena dampak dari risiko, persamaan risiko dapat digambarkan sebagai berikut : Ancaman (kondisi) + dampak (konsekuensi) = risiko, |langkah 4 dan 5| + |langkah 6| = risiko, maksudnya adalah langkah 4 merupakan pemetaan lingkungan risiko asset informasi + langkah 5 adalah output dari langkah 4 yang merupakan hasil pengembangan scenario ancaman dari area of concern + langkah 6 adalah mengidentifikasi risiko merupakan konsekuensi dari scenario ancaman (kondisi) = risiko. Pada tabel 1.5 *impact area* terdapat kolom penilaian priority untuk mengukur criteria semua aset informasi yang penting yang terdapat pada sistem informasi akademik, sedangkan *low, medium* dan *high* untuk menentukan nilai risiko pada setiap impact area.

3.7 Menganalisa Risiko

Pada langkah 7 (tujuh), diberikannya nilai kualitatif kepada jangkauan sejauh mana Sistem Informasi Akademik diperngaruhi oleh ancaman dengan cara menghitung nilai risiko untuk tiap risiko terhadap setiap asset informasi. Penilaian ini digunakan untuk menentukan risiko mana yang membutuhkan langkah mitigasi secepatnya dan untuk memprioritaskan tindakan mitigasi secepatnya dan untuk memprioritaskan tindakan mitigasi pada langkah 8 (delapan). Pada penilaian risiko terstruktur, akan dilakukan aktivitas yang memberikan langkah sistematis untuk menganalisa bagaimana Sistem Informasi Akademik terpengaruh oleh suatu risiko. Pada aktivitas ini akan dihasilkan nilai risiko relative. Nilai risiko relative dihasilkan dari menghitung jangkauan dari dampak yang dihasilkan suatu risiko terhadap perusahaan terhadap nilai relative kepentingan pada macam-macam *Impact Area*. Dengan kata lain, jika area reputasi merupakan area terpenting dari organisasi dan konsekuensi dari risiko menghasilkan dampak yang besar bagi area reputasi, harus diambil tindakan yang memastikan risiko ini di mitigasi. Dengan menggunakan criteria-criteria ini, pastikan bahwa risiko diberikan nilai yang mengacu pada *organizational drivers*.

3.8 Memilih Pendekatan Mitigasi

Pada langkah 8 (delapan) ini, ditentukan risiko yang dimitigasi, disediakan tabel *risk score* untuk menentukan risiko dimitigasi, dibiarkan atau diterima oleh organisasi. langkah 8 kegiatan pertama yang dilakukan adalah memilah masing-masing risiko yang telah identifikasi dengan skor risikonya. Mengkategorikan risiko secara teratur akan membantu mulai membuat keputusan tentang status mitigasi.

Ada banyak cara bagi organisasi atau perusahaan untuk mengkategorikan risikonya. Salah satu metode sederhana adalah memulai

dengan menyortir risiko dalam urutan dari tertinggi ke terendah. Kemudian pisahkan risiko menjadi tigakolam dengan jumlah risiko yang sama. Risiko dengan skor tertinggi harus di yang pertama (Pool 1), risiko dengan rentang skor tertinggi berikutnya di kedua (Pool 2), dan skor terendah dalam keempat (Pool 4). Langkah selanjutnya adalah pengembangan strategi mitigasi risiko. Untuk setiap risiko dengan pendekatan *mitigate*, maka perlu dibuat suatu strategi untuk mitigasi risiko tersebut. Dalam mengembangan strategi tersebut, perlu diperhatikan *container* dimana control akan diterapkan dan *residual risk* (risiko yang tersisa) setelah control diimplementasikan. Residual risk yang ada harus berada dalam tingkat yang dapat ditoleransi oleh organisasi atau perusahaan.

Pendekatan mitigasi pool 1 adalah *mitigate* maksudnya adalah tindakan yang diambil jika score relative risiko sangat tinggi, sehingga perlakuan risiko langsung dipimpin oleh Direktur terkait. Pool 2 adalah *mitigate/defer* maksudnya adalah tindakan yang diambil jika score relative risiko cukup tinggi, sehingga perlakuan risiko setingkat dan perlu perhatian Direktur terkait atau cukup menggunakan SOP yang ada, atau SOP baru, atau perlu perbaikan SOP guna memastikan keefektifannya sebagai *risk control*. Pool 4 adalah *accept* maksudnya adalah jika score relative risiko rendah sehingga tidak perlu perlakuan risiko tertentu, cukup dimonitor saja.

4. Referensi

Abbass, W., Baina, A., & Bellafkih, M. (2016). Improvement of information system security risk management. 4*th* IEEE *International Colloquium on Information Science and Technology (CiSt)* (pp. 182-187). Tangier-Assilah, Marocco: IEEE.

Al-Ahmad, W., & Mohammed, B. (2015). A code of practice for effective information security risk management using COBIT 5. 2015 *Second International Conference on Informastion Security and Cyber Forensics (InfoSec)* (pp.145-151). Cape Town, South Africa: IEEE.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W.R. (2007*). Introduction OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* United State: Carnegie Mellon University.

C. Alberts, A. Dorofee, J. Stevens, and C. Woody. (2005). *Introduction to the OCTAVE Approach*. PA 15213-3890. Versi 1, Carnegie Mellon Institute.

Damayanti, Vani. (2015). Manajemen Risiko Aset Informasi Sistem Langgeng Pada Bank BPR Taeh Baruh Kec Payakumbuh Dengan Menggunakan Metode Octave Allegro. *Ancaman Sistem Informasi*. Pekanbaru: Uin Suska Riau.

Damayanti, Vani. (2015). Manajemen Risiko Aset Informasi Sistem Langgeng PAda Bank BPR Taeh Baruh Kec Payakumbuh Dengan Menggunakan Metode Octave Allegro. *Manajemen Risiko Aset Informasi Berdasarkan Octave Allegro*. Pekanbaru: Uin Suska Riau.

Ermatita. (2016). Sistem Informasi. *Jurnal Sistem Informasi (JSI)*- Volume 8 Nomor 1, 1-12

Gibson, D. (2011). *Managing Risk In Information System*. Jones & Bartlett Learning.

Harris, I., Tarigan, M. L., & Mawlan, S. (2013). *Analisis Manajemen Risiko pada Implementasi Sistem Informasi Keamanan di PT. Pupuk Sriwidjaja dengan framework COBIT 4.1*. Palembang: STIMIK MDP.

Jakaria, D. A., Dirgahayu, R. T., & Hendrik. (2013). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi menggunakan Metode Octave Allegro. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, 37-42.

Kang, Y., & Liu, R. (2016). Development of a rail breaking risk management information system. 3rd *International Conference on Systems and Informatics (ICSAI)* (pp.492-496). Shanghai China:IEEE.

Lokobal, A, Sumajouw, M.D. & F. Sompie, B., 2014. *Manajemen Risiko Pada Perusahaan Jasa Pelaksanaan Konstruksi Di Provinsi Papua (Study Kasus di Kabupaten Sarmi)*, Volume 4, pp. 109-118.

Masky, M., Young, S. S., & Shoe, T. Y. (2015). A Novel Risk Identification

Framework for Cloud Computing Security. *2nd International Conference in Information Science and Security (ICISS)* (pp. 61-64). USA: IEEE.

Nurochman, A. (2014). Manajemen Risiko Sistem Informasi perpustakaan (Studi Kasus di Perpustakaan Universitas Gadja Mada Yogyakarta). *Berkala Ilmu Perpustakaan dan Informasi – Volume X Nomor 2,* 1-13.

Pradana, Y. A & Rikumahu, B., 2014. *Penerapan Manajemen Risiko terhadap Perwujudan Good Corporate Governance pada Perusahaan Asuransi,* Desember, Volume 13, pp. 195-204.

Rilyani, A. N., Firdaus, Y., & Jatmiko, D. D. (2015). *Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus :i-Gracias Telkom University).* Bandung: Universitas Telkom.

Rosini, R, Meutia., M, Badollahi. (2016). *Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allegro*. Jurnal Pustakawan Indonesia - Volume 14 Nomor 1, 1-9.

Wijanarka, H. (2014). IT risk management to Support the realization of IT value in public organization. 2014 *International Conference on ICT For Smart Society (ICISS)* (pp. 113-117). Bandung: IEEE