ANALISIS RISIKO KEAMANAN TEKNOLOGI INFORMASI MENGGUNAKAN OCTAVE ALLEGRO

Hidayatul Ikhsan*[1] , Nanda Jarti [*2]
STT Ibnu Sina; Jalan Tengku Umar-Lubuk Baja
[3]Program Studi Teknik Industri, STT Ibnu Sina, Batam
e-mail: *[1]hidayatul.ikhsan68@gmail.com, *[2] nandaluthan@gmail.com

ABSTRAK

Informasi merupakan aset yang penting bagi lembaga perguruan tinggi yang harus dilindungi dan diamankan, sehingga jaminan ketersediaan informasi yang aman dan terpercaya dapat digunakan bagi lingkungan eksternal maupun internal. Saat ini belum banyak perguruan tinggi yang melakukan penilaian risiko terhadap sistem informasi yang digunakan. Dengan demikian jika terdapat gangguan pada sistem informasi maka dapat mengganggu keberlangsungan dari proses lembaga yang bersangkutan. Risiko merupakan sebuah kejadian yang tidak diinginkan dimana dihasilkan dari sebuah kejadian atau peristiwa sehingga berdampak merugikan dan hasilnya tidak pasti. Dalam mengidentifikasi dan mengevaluasi dari risiko keaman sebuah aset informasi dapat digunakan metode OCTAVE allegro untuk memberikan gambaran penanganan dari risiko sistem yang terjadi. Hasil dari penilaian risiko ini hanya sampai tahapan ketiga yaitu menentukan Identify Threats dimana tahap pertama estabilsh drivers, yaitu menetapkan apa yang menjadi arahan organisasi. Tahap kedua Membuat profile assets, yaitu membuat profil aset yang telah dimiliki organisasi. Tahap ketiga identify threats, yaitu mengidentifikasi ancaman untuk setiap aset informasi dalam kontek wadahnya.

Kata kunci : Aset, Risiko, Keamanan, Octave Allegro

ABSTRACT

Information is an important asset for higher education institutions that must be protected and secured, so that the guarantee of the availability of safe and reliable information can be used for the external and internal environment. Currently there are not many universities that conduct risk assessments of the information systems used. Therefore, if there is a disruption in the information system, it can interfere with the sustainability of the process of the institution concerned. Risk is an undesirable event that results from an event or event that has an adverse impact and the results are uncertain. In identifying and evaluating the security risks of an information asset, the OCTAVE Allegro method can be used to provide an overview of the handling of system risks that occur. The results of this risk assessment are only up to the third stage, which is determining Identify Threats where the first stage is estabilsh drivers, which determining what is the direction of the organization. The second stage Creating a profile assets, which is to create an asset profile that has been owned by the organization. The third stage of identifying threats, namely identifying threats to each information asset in the context of the container.

Keywords : Assets, Risks, Security, Octave Allegro

1. PENDAHULUAN

Teknologi informasi pada saat sekarang menjadi hal yang sangat penting karena sudah banyak perguruan tinggi yang menerapkan teknologi informasi sebagai pendukung dalam meningkatkan kualitas informasinya. Seperti halnya sistem informasi merupakan penunjang

utama dalam melakukan pengolahan data untuk menghasilkan informasi saat ini. [12], data mempunyai peran yang sangat penting dalam sebuah sistem informasi karena merupakan salah satu komponen sistem informasi, data yang digunakan merupakan sebuah data yang telah diorganisir menjadi suatu informasi dan kemudian akan diterima sebgai pengetahuan dan digunakan untuk mengambil keputusan. Begitu juga lembaga perguruan tinggi pemanfaatan sistem informasi telah menjadi kebutuhan pokok. Tetapi tidak selamanya pemanfaatan teknologi informasi dalam pengelolaan sebuah sistem informasi sesusai dengan yang diharapkan.

Dalam penggunaannya terkadang muncul berbagai risiko yang dapat mengganggu keberlansungan sistem informasi sehingga dapat mengakibatkan kerugian bagi perguruan tinggi. Menurut Stoneburner, dikutip oleh [10], menyebutkan bahwa risiko adalah dampak negatif yang diakibatkan dengan adanya kerentanan *(vulnerability)*, berdasarkan dari probalitas maupun dampak kejadian.

Dengan melakukan penilaian risiko teknologi informasi diharapkan dapat mengurangi dampak dari kerusakan yang bisa berupa, dampak dari finansial, menurunya keperyayaan pengguna akibat sistem yang tidak aman, dan penundaan proses pengambilan keputusan.

Untuk itu perlu dilakukan penilaian risiko terhadap kerawanan informasi. Salah satu metode yang dapat digunakan untuk penilaian dan analisis risiko teknologi informasi adalah menggunakan OCTAVE *(Operationally Critical Threat, Assets and Vulnerability Evaluation)*. [1], OCTAVE merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamanan sistem informasi berbasis risiko.

Penelitian ini memfokuskan pada analisis, identifiasi dan penilaian risiko keamanan sistem informasi dosen pada perguruan tinggi menggunakan metode OCTAVE Allegro.

2. METODE PENELITIAN

2.1. Pengertian sistem informasi

[6], sistem informasi adalah suatu sistem didalam suatu organisasi yang mempertemukan kebutuhan pengelolaan transaksi harian, mendukung operasi, bersifat manajerial, dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tententu dengan laporan – laporan yang dibutuhkan.

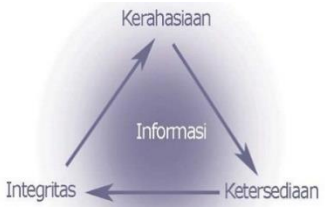
Sistem informasi merupakan kumpulan komponen yang saling berintaraksi satu dengan yang lainnya untuk mengolah input berupa data menjadi informasi yang bertujuan untuk mencapai tujuan bersama.

2.2. Risiko

[10], menyebutkan bahwa risiko adalah dampak negatif yang diakibatkan dengan adanya kerentanan *(vulnerability)*, berdasarkan dari probalitas maupun dampak kejadian. Jadi risiko merupakan sebuah kejadian yang tidak diinginkan dimana dihasilkan dari sebuah kejadian atau peristiwa sehingga berdampak merugikan dan hasilnya tidak pasti.

2.3. Keamanan Informasi

[4]**,** keamanan informasi memuat beberapa aspek yang penting, seperti *Confidentiality* (kerahasiaan), *Integrity* (integritas), *Integrity* (integritas) yang terlihat pada gambar berikut.



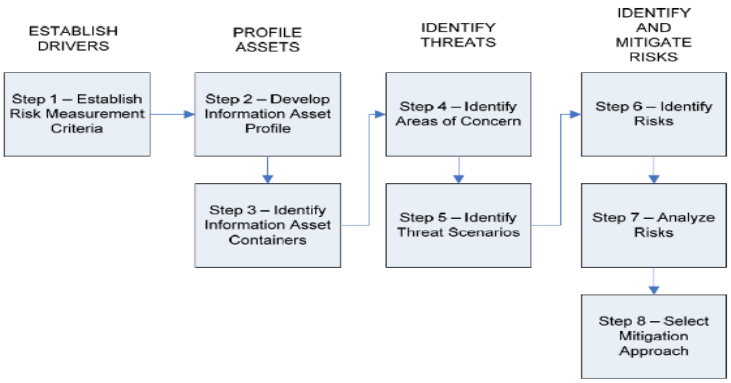
Gambar 1 Aspek Keamanan Sistem Informasi

2.4. Metode OCTAVE Allegro

Metode OCTAVE merupakan singkatan dari *Operationally Critical Threat, Asset, and Vilnerability Evaluation*. [4]**,** OCTAVE merupakan metodelogi yang digunakan untuk mengidentifikasi dan mengevaluasi dari risiko keaman sebuah informasi. OCTAVE melakukan penilaian risiko berdasarkan pada tiga prinsip dasar administrasi keamanan, yaitu : 1) *confidentiality*, 2) *integrity*, 3) *availability*.

Metode OCTAVE memiliki tiga varian yaitu , OCTAVE, OCTAVE-S. OCTAVE *Allegro*. OCTAVE Allegro tidak dimaksudkan untuk menggantikan metode OCTAVE yang sebelumnya. Ketiga metode tersebut bukanlah jenis metode yang saling melengkapi, atau menggantikan satu sama lainnya. Melainkan penggunaan dari ketiga metode tersebut dimaksudkan untuk memenuhi kebutuhan yang spesifik dari pengguna OCTAVE yang ingin melakukan penilaian risiko. Fokus utama dari metode OCTAVE Allegro sendiri adalah pada aset informasi, dalam konteks yaitu bagaimana mereka digunakan, di manan mereka disimpan, diangkut, diproses dan bagaimana keadaannya jika terkena ancaman, kerentanan, dan gangguan sebagai hasil yang ditimbulkan. Selain itu yang termasuk dalam lampiran OCTAVE Allegro didukung dengan panduan lembaran kerja berupa kuensioner.

Tahapannya yaitu, Membangun *drivers*, Membuat profil aset, Mengidentifikasi ancaman, Mengidentifikasi dan mengurangi risiko.



Gambar 2 Langkah – langkah metode OCTAVE Allegro

2.5. Tahapan Penilaian Risiko

Penelitian ini mendeskripsikan hasil dari setiap langkah atau lembar kerja yang diadopsi dari metode OCTAVE *Allegro* dalam menilai risio keamanan aset informasi di STKIP PGRI. Pada penelitian ini menggunakan metode penelitian kualitatif, yaitu dengan observasi dan wawancara yang bertujuan untuk mengumpulkan informasi secara rinci, mengidentifikasi masalah, mengungkap fakta, keadaan fenomena dan keadaan yang terjadi saat penelitian berjalan.

[4], setiap tahapan dari delapan tahapan diatas, maka dirinci lagi menjadi beberapa aktivitas penilaian risiko yang akan dilakukan. Untuk memudahkan implementasinya maka OCTAVE *Allegro* memberikan panduan berupa *worksheet* 1 sampai 10 seperti tabel 1.

Tabel 1. Tahapan OCTAVE *Allegro*

Tahap	Aktivitas	Output	*Worksheet*/Acuan
1	Membangun Kriteria Pengukuran Risiko	• Kriteria pengukuran risiko terhadap arahan organisasi • Peringkat area dampak dari yang paling penting hingga yang tidak penting	*Allegro Worksheet* 1-5 dan 6-7
2	Mengembangkan Profil Aset Informasi	Profil aset informasi kritis	*Allegro Worksheet* 8

Tahap	Aktivitas	Output	*Worksheet*/Acuan
3	Mengidentifikasi Kontainer dari Aset Informasi	Pemetaan lingkungan risiko aset informasi	*Allegro Worksheet* 9a, 9b, dan 9c
4	Mengidentifikasi *area of conceren* (area yang bermasalah)	Peta lingkungan risiko aset informasi	*Allegro Worksheet* 10
5	Mengidentifikasi Skenario ancaman	• Informasi detail dan hasil pengembangan skenario ancaman dari *area of concern* • Daftar risiko aset informasi	• Output tahap 4 (*Information Asset Risk Environment Maps*) • *Worksheet* 10 • *Information Asset Risk Worksheets*
6	Mengidentifikasi Risiko	Konsekuensi dari skenario ancaman **Ancaman (kondisi) + Konsekuensi (dampak) = Risiko** **[Langkah 4=5] + [langkah 6] = Risiko**	*Information Asset Risk Worksheet*
7	Analisis Risiko	• Tabel area dampak • Tabel skor risiko	• *Risk measurement Criteria* • *Information Asset Risk Worksheet* 10
8	Memilih Pendekatan Mitigasi	• Matriks risiko relatif • Tingkat kerawanan informasi • Mitigasi untuk semuas daftar risiko • Strategi mitigasi untuk setiap risiko yang telah diputuskan untuk dilakukan mitigasi	

3. HASIL DAN PEMBAHASAN

Tahapan pertama yang dilakukan dalam penilaian risiko keamanan informasi dimulai dengan menghubungi pihak – pihak pengelola di devisi IT untuk mendapatkan data – data yang diperlukan. Tahap selanjutnya adalah melakukan wawancara untuk mendapatkan informasi mengenai aset informasi kritis bagi sistem informasi dosen STKIP PGRI.

Langkah 1 – Membangun Kriteria Pengukuran Risiko

Aktivitas 1 – Penentuan *Impact Area*

Pada aktivitas ini terdapat enam *impact area* yang kemudian dilakukan penentuan nilai kualitatifnya masing – masing (*low, moderate, high*). Penentuan ini berdasarkan besarnya dampak risiko yang terjadi bagi aset informasi STKIP PGRI. Tabel 1 berisi hasil penentuan *impact area* – reputasi dan kepercayaan pengguna.

Tabel 2 *Impact Area* – Reputasi dan Kepercayaan Pengguna

Reputasi dan kepercayaan pengguna	Reputasi	LOW	MODERATE	HIGH
		Reputasi sedikit terpengaruh; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan.	Reputasi terkena dampak buruk, dan dibutuhkan usaha dan biaya untuk perbaikan.	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki.

Aktivitas 2 – Pentuan skala prioritas *impact area*

Impact area yang lebih penting akan memiliki nilai skala prioritas yang lebih besar. Hasil dari aktivitas akan digunakan nantinya dalam penilaian risio untuk mengembangkan nilai risiko relatif yang dapat membantu STKIP PGRI dalam menangani risiko yang telah diidentifikasi dalam penilaian.

Tabel 3. Skala prioritas untuk *impact area*

Priority	***Impact Area***
6	**Reputasi dan kepercayaan pengguna**
5	**Finansial**
3	**Produktivitas**
1	**Keamanan dan kesehatan**
4	**Denda dan penalti**
2	**Pengelolaan risiko dan aset**

Langkah 2 – Mengembangkan *Information Asset Profile*

Dalam menentukan aset informasi apa saja yang kritikal bagi STKIP PGRI, penilaian akan dilakukan dengan berfokus kepada *core process*. Dimana *core process* pada STKIP PGRI akan dilakuan hanya untuk sistem informasi dosen. Dari proses sistem informasi dosen, yang termasuk di dalam *core process* adalah proses yang dimulai dari memberikan kemudahan bagi dosen dalam melakukan aktivitas akademik dan dalam proses belajar mengajar. Pada tabel berikut ini akan diberikan informasi mengenai sistem informasi dosen, pengguna sistem merupakan orang yang menggunakan sistem, dan *core process*.

Tabel 4. Sistem Informasi Dosen

Sistem	**Pengguna**	***Core* Process**
Sistem Informasi Dosen : merupakan sistem informasi yang digunakan untuk membantu para dosen dalam menerima dan meng*update* informasi dan dapat memberi kemudahan untuk melakukan aktivitas akademik, serta membantu dalam proses belajar mengajar.	Dosen	1. Menerima dan *update* informasi. 2. belajar dan mengajar.

Mengacu pada *core process*, maka aktivitas ini dimulai dengan memilih aset informasi yang berhubungan atau digunakan dalam sistem informasi dosen. Aset informasi yang telah ditentukan sebagai aset informasi kritikal, maka akan dicatat dalam *critical information asset worksheet* yang telah disediakan oleh metode OCTAVE *Allegro*. Aset informasi yang dipilih harus mempertimbangkan hal – hal berikut :

1. Aset informasi yang digunakan dalam kegiatan operasional pekerjaan sehari – hari.
2. Aset informasi yang jika hilang, akan mengganggu kemampuan sistem informasi dosen untuk berkontribusi dan menyelesaikan tujuannya.

Dari hasil pertimbangan diatas, maka didapatkan hasil melalui wawancara terdapat informasi yang dapat dikategorikan sebagai aset informasi yang penting, yaitu:

1. Presensi Dosen dan Mahasiswa
2. Jadwal Kuliah
3. Bimbingan Akademi
4. Nilai Kuliah
5. Kalender Akademik
6. Informasi Matakuliah
7. Inquiry Status Mahasiswa
8. Setup Pengumuman
9. Pengumuman
10. Setup Dokumen
11. Daftar Dokumen
12. LOG Aktifitas
13. Presensi Dosen dan Mahasiswa
14. Nilai
15. Preference

Dari aset informasi yang telah diidentifikasi, langkah selanjurnya adalah berfokus terhadap aset informasi yang benar – benar kritikal bagi sistem informasi dosen. Dimana dengan cara menanyakan lansung kepada koresponden melalui wawancara, dari aset informasi paling penting yang telah sebutkan mana saja yang termasuk dalam kritikal terhadap sistem informasi dosen dan mengacu kepada beberapa kriteria, aset yang jika terjadi dapat menyebabkan dampak yang besar (*high*) bagi sistem informasi dosen jika terjadi hal – hal seperti berikut:

1. Aset informasi kritis tersebut diakses oleh orang yang tidak berwenang.
2. Aset informasi kritis tersebut dimodifikasi tanpa otoritas.
3. Aset informasi tersebut hilang atau hancur

Dari poin – poin diatas dan berdasarkan hasil dari wawancara, maka dapat disimpulkan aset informasi kritikal apa saja yang harus dijaga oleh divisi IT STKIP PGRI, sebagai berikut:

1. Presensi Dosen dan Mahasiswa
2. Bimbingan Akademik
3. Nilai Kuliah
4. Setup Pengumuman
5. Setup Dokumen
6. Preference

Langkah selanjutnya yaitu informasi yang telah dikumpulkan lalu disimpan dan dilengkapi pada *worksheet*, dimana pelengkapan *worksheet* tersebut dilakukan dengancara melakukan wawancara.

Dalam *information asset profile*, informasi dilihat dalam lima bagian yaitu, *rationale of selection* adalah alasan – alasan mengapa informasi tersebut menjadi kritikal bagi sistem informasi dosen, *description* adalah penjelasan data penting apa saja yang terdapat dalam informasi tersebut, *owner* adalah pemilik dari informasi tersebut, *security requirement* untuk mengetahui informasi tersebut terbagi dalam tiga bagian, yaitu *confidentiality*, *integrity*, dan *availability*, serta *most important security requirement* dimana memilih *security requirement* manakah yang paling diutamakan. Tabel 4 berisi contoh *Information asset profiling* – Presensi Dosen & Mahasiswa.

Tabel 5. *Information asset profiling* – Presensi Dosen & Mahasiswa

Critical Asset		Presensi Dosen & Mahasiswa
Rationale for Selection		Presensi dosen dan mahasiswa merupakan absensi kelas yang berhubungan dengan status mata kuliah yang diambil oleh mahasiswa. Dapat ikut/tidaknya seorang mahasiswa dalam ujian akhir semester ditentukan oleh absensi.
Description		Aset ini terdiri dari tahun akademik, matakuliah, waktu kuliah, tempat,nama dosen, SKS, tanggal absen, NIM, status absen.
Owner		Manajer, devisi IT STKIP PGRI
Security Requirements	*Confidentiality*	Informasi presensi dosen & mahasiswa bersifat penting mahasiswa dan jurusan. Bagian administrasi mahasiswa menggunakan informasi untuk menentukan mana yang bisa ikut ujian atau tidak.
	Integrity	Informasi ini harus diisi oleh dosen setiap pertemuan dan harus sesuai dengan absensi dikelas.
	availability	Informasi ini harus tersedia bagi dosen, jurusan dan administrasi kemahasiswaan.
Most Important Security Requirement		***Integrity*** Alasan: informasi ini harus akurat dan sesuai dengan kondisi dikelas. Dalam absensi terdapat batas ketidak hadiran mahasiswa sesuai dengan sks. Jika ketidak hadiran mahasiswa melebihi ambang batas, maka mahasiswa tersebut tidak dapat mengikuti ujian. Maka dari itu informasi ini harus akurat.

Langkah 3 – Identifikasi *Information Asset Containers*

Pada langkah 3, kita mengidentifikasikan *information asset containers*, dimana aktifitas ini dimulai dengan wawancara. *Information asset containers* adalah kontainer atau tempat dimana aset informasi disimpan, dipindahkan atau diproses. Dengan menggunakan *worksheet information asset risk environment map*, untuk mengidentifikasi kontainer dimana aset informasi berada, yang dibagi dalam tiga kategori, yaitu:

1. ***Technical*** – sebuah perangkat keras, perangkat lunak atau sistem yang dibawah kontrol perusahaan (internal), ataupun diluar kontrol perusahaan (eksternal).
2. ***Physical*** – lokasi fisik atau dokumen yang dibawah kontrol perusahaan (internal), ataupun diluar kontrol perusahaan (eksternal).
3. ***People*** – siapa saja yang mengetahui informasi yang dibawah kontrol perusahaan (internal), ataupun diluar kontriol perusahaan (eksternal).

Adapun penjelasan dari langkah berikut ini berisi contoh *Information Asset Containers* - Presensi Dosen & Mahasiswa.

Tabel 6. *Information Asset Risk Environment Map (Technical)*

Presensi Dosen & Mahasiswa	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	***Owner(s)***
Aplikasi: Presensi Jurusan Presensi dosen & mahasiswa di akses dan diproses untuk pendataan kehadiran mahasiswa dikelas.	Administrasi Kemahasiswaan
External	
Container Description	***Owner(s)***
Aplikasi: Presesnsi Kuliah Presensi dosen & mahasiswa di akses untuk mengisi daftar kehadiran setiap mahasiswa sesuai dengan mata kuliah, tanggal, waktu kuliah, dsb.	Dosen

Tabel 7. *Information Asset Risk Environment Map (Physical)*

Presensi Dosen & Mahasiswa	
Information Asset Risk Environment Map (Physical)	
Internal	
Container Description	***Owner(s)***
Infrastruktur : *network*, server Seluruh data pada Sistem informasi dosen didukung oleh infrastruktur yang saling terintegrasi supaya data dapat saling sinkronisasi.	Devisi It
Laporan – laporan yang terkait absensi kelas yang telah dicetak melalui presensi jurusan untuk keperluan internal.	Administrasi Kemahasiswaan
External	
Container Description	***Owner(s)***
Hasil cetak absensi mahasiswa melalui presensi dosen & mahasiswa.	Dosen

Tabel 8. *Information Asset Risk Environment Map (People)*

Presensi Dosen & Mahasiswa	
Information Asset Risk Environment Map (People)	
Internal	
Container Description	***Owner(s)***
Staff administrasi kemahasiswaan	Administrasi Kemahasiswaan
Staff IT	Devisi IT
External	
Container Description	***Owner(s)***
Dosen	Dosen

Langkah 4 - Identifikasi *Areas of Concern*

Langkah empat digunakan untuk menjabarkan aktivitas – aktivitas untuk mengidentifikasi *areas of concern*. Adapun aktivitas – aktivitas *areas of concern* adalah sebagai berikut.

1. Melakukan review terhadap setiap *container* yang telah dibuat untuk melihat *areas of concern* yang potensial.
2. Medokumentasikan setiap *areas of concern* yang diidentifikasikan kedalam *information asset risk worksheet*.

Pada *areas of concern* dapat dibagi menjadi dua bagian sesuai dengan *container* yang telah dibuat yaitu *human error* yang dilakukan oleh pengguna aplikasi dan dari segi IT. Tabel 8 berisi contoh identifikasi *areas of concern* pada presensi dosen & mahasiswa.

Tabel 9. *Areas of Concern* – Presensi Dosen & Mahasiswa

No	***Areas of Concern***
1	Kesalahan dosen dalam melakukan input absensi pada aplikasi presensi kuliah.
2	Penyebaran hak akses (*password*) terhadap aplikasi sistem informasi dosen yang dapat mengakses presensi mahasiswa oleh yang memiliki akses.
3	Ketika dosen mengakses sistem informasi dosen melalui komputer umum, terdapat pihak ketiga yang mendapat akses terhadap data presensi dosen dan mahasiswa.
4	*Bug/error* yang terjadi pada aplikasi presensi dosen dan mahasiswa yang muncul ketika staff devisi IT melakukan *maintenance*.
5	*Bug/error* yang terjadi pada sistem informasi dosen yang muncul ketika staff devisi IT melakukan *maintenance*.
6	Pemanfaatan celah keamanan sistem informasi dosen oleh pihak dalam/luar.
7	Staf devisi IT memasukan script yang dapat membahayakan sistem informasi dosen.

Langkah 5 - Identifikasi *Threat Scenarios*

Dalam langkah ini, *areas of concern* diperluas menjadi *threat scenario* yang memberikan gambaran secara rinci mengenai *property* dari *trheat*. Adapun hasil dari skenario ancaman didapatkan dengan menjelaskan antara lain *Actor, Means, Motives, Outcome, Security requirements.*

Dari setiap skenario ancaman yang didapatkan maka dapat dilihat bagai mana solusi yang harus diambil untuk mencegah risiko tersebut terjadi, solusi akan diambil dengan cara melihat bagaimana risiko tersebut dapat terjadi dan motif dari pelaku ketika melakukan risiko tersebut.

Adapun aktivitas – aktivitas yang harus dilakukan dalam identifikasi *threat scenario* adalah sebagai beriut:

1. Melengkapi *information asset risk worksheets* untuk setiap *threat scenarios* umum yang diidentifikasikan.
2. Menentukan probabilitas kedalam deskripsi *threat scenario* yang telah dibuat pada *information asset risk worksheets*.

Tabel 9 merupakan contoh *Properties of Threat* hasil pengembangan dari *areas of concern* Presensi Dosen & Mahasiswa.

Tabel 10. *Properties of Threat* – Presensi Dosen & Mahasiswa

1	***Area of Concern***	***Threat of Properties***	
	Kesalahan dosen dalam melakukan input absensi pada aplikasi presensi kuliah	***1. Actors***	Dosen
		2. Means	Dosen menggunakan aplikasi presensi kuliah
		3. Motives	Dosen tidak sengaja melakukan kesalahan meng input absensi mahasiswa (*accindental)*
		4. Outcome	*Loss*
		5. Security Requirements	Memberikan pemahaman untuk hati-hati dalam penginputan absensi mahasiswa
2	***Area of Concern***	***Threat of Properties***	
	Penyebaran hak akses (*password*) terhadap aplikasi sistem informasi dosen yang dapat mengakses presensi mahasiswa oleh yang memiliki akses	***1. Actors***	Dosen
		2. Means	Akses terhadap sistem informasi dosen
		3. Motives	Dosen secara sengaja/tidak sengaja membagikan hak akses (*accindental, deliberate*)
		4. Outcome	*Disclosure, Modification, Interruption*
		5. Security Requirements	Memberikan penyuluhan untuk menjaga kerahasiaan hak akses dan memberikan hukuman bagi yang sengaja menyebarkan hak akses yang dimiliki
3	***Area of Concern***	***Threat of Properties***	
	Ketika dosen mengakses sistem informasi dosen melalui komputer umum, terdapat pihak ketiga yang mendapat akses terhadap data presensi dosen dan mahasiswa	***1. Actors***	Tidak diketahui
		2. Means	Dosen yang lupa *log out* setelah selesai akses sistem informasi dosen
		3. Motives	*Accidental* (tidak sengaja)
		4. Outcome	*Disclosure*
		5. Security Requirements	Dilakukan *reset pasword* dalam periode tertentu
4	***Area of Concern***	***Threat of Properties***	
		1. Actors	Staff devisi IT

	Bug/error yang terjadi pada aplikasi presensi dosen dan mahasiswa yang muncul ketika staff devisi IT melakukan *maintenance*	***2. Means***	Akses aplikasi presensi dosen dan mahasiswa dalam modifikasi/perbaikan
		3. Motives	Terjadi karena *human error* (*accidental*)
		4. Outcome	*Disclosure, Modification, Interruption*
		5. Security Requirements	Diperketatnya pengujian dan QA (*Quality Assurance*) sebelum digunakan
5	***Area of Concern***	***Threat of Properties***	
	Bug/error yang terjadi pada sistem informasi dosen yang muncul ketika staff devisi IT melakukan *maintenance*	***1. Actors***	Staff devisi IT
		2. Means	Akses sistem informasi dosen dan mahasiswa dalam modifikasi/perbaikan
		3. Motives	Terjadi karena *human error* (*accidental*)
		4. Outcome	*Disclosure, Modification, Interruption*
		5. Security Requirements	Diperketatnya pengujian dan QA (*Quality Assurance*) sebelum digunakan
6	***Area of Concern***	***Threat of Properties***	
	Pemanfaatan celah keamanan sistem informasi dosen oleh pihak dalam/luar	***1. Actors***	Tidak diketahui
		2. Means	Pihak ketiga mengetahui celah keamanan sistem informasi dosen dan memanfaatkannya
		3. Motives	*Deliberate* (sengaja)
		4. Outcome	*Disclosure, Modification, Interruption, Loss*
		5. Security Requirements	Peningkatan uji QA (*Quality Assurance*) terhadap sistem informasi dosen yang dilakukan oleh staff devisi IT
7	***Area of Concern***	***Threat of Properties***	
	Staf devisi IT memasukan script yang dapat membahayakan sistem informasi dosen.	***1. Actors***	Staff IT
		2. Means	Staff devisi IT yang memiliki akses terhadap *source code*
		3. Motives	*Deliberate* (sengaja)
		4. Outcome	*Disclosure, Modification, Interruption, Loss*
		5. Security Requirements	Penerapan QA (*Quality Assurance*) terhadap *source code* yang dihasilkan pada saat *maintenance*

4. KESIMPULAN

Penilaian risiko pada dasarnya merupakan proses dari identifikasi terhadap aset informasi, keamanan dan ancaman. Metode OCTAVE Allegro merupakan salah satu metode penilaian risiko teknologi informasi yang bisa diterapkan pada perguruan tinggi dan difokuskan kepada aset informasi kritis bagi keberlansungan organisasi dalam mencapai tujuannya.
Dalam penilaian risiko dapat memberikan sebuah gambaran kemungkinanan adanya ancaman terhadap aset informasi yang kritikal dan mengambil langkah – langkah pencegahan yang tepat agar dapat meminimalkan kemungkinan ancaman tersebut terjadi.

Berdasarkan penilaian risiko sampai fase *Identify Threats* menggunakan OCTAVE Allegro maka didapatkan sebuah gambaran dari setiap aset informasi yang kritis yang menentukan batasan – batasan yang jelas untuk aset, mengidentifikasi syarat dari keamanan aset tersebut dan mengidentifiasi semua wadahnya bagi sistem informasi dosen pada STKIP PGRI.

5. SARAN

1. Melakukan evaluasi keamanan risiko aset informasi dengan menggunakan metode OCTAVE *Allegro* secara berkala, setidaknya satu tahun sekali, agar dapat mengetahui kebutuhan dan kelemahan dari teknologi informasi yang digunakan.
2. Untuk penelitian berikutnya, ruang lingkup penulisan dapat menggunakan area lain di STKIP PGRI, seperti aset informasi bagian sistem informasi mahasiswa atau pada devisi IT.

DAFTAR PUSTAKA

Ahmad, D (2013). "*Manajemen Risiko Sistem Informasi Akademik pada Perguruan tinggi Menggunakan Metoda Octave Allegro*". SNATI. Hal.37-42.

Caralli, R. A. (2007). "*Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*". Software Engineering Institute. Hal.2-90.

Hutahaean, J. (2014). "*Konsep Sistem Informasi*", Yogyakarta; Deepublish. Hal.4-5.

Nugraha, U (2016). "*Manajemen Risiko Sistem Informasi pada Perguruan Tinggi Menggunakan Kerangka kerja NIST SP 800-300*". Seminar Nasional Telekomunikasi dan Informatika. Hal.121-126.

Rosini (2015), "*Penilaian Risiko Kerawanan Informasi dengan Menggunakan Metode OCTAVEAllegro*". Jurnal Pustakawan Indonesia. Vol.14, Hal.14-22.

Setyabudhi, A. L. (2017). Perancangan Sistem Informasi Pengolahan Data Absensi dan Pengambilan Surat Cuti Kerja Berbasis Web. *JR: JURNAL RESPONSIVE Teknik Informatika*, *1*(1).

Veza, O. (2017). Perancangan Sistem Informasi Inventory Data Barang Pada Pt. Andalas Berlian Motors (Studi Kasus: PT Andalas Berlian Motors Bukit Tinggi). *Jurnal Teknik Ibnu Sina JT-IBSI*, *2*(2).

Veza, O. (2016). Simulasi Pengendalian Persedian Gas Menggunakan Metode Monte Carlo Dan Pola Lcm (Studi Kasus Di PT PKM Group Cabang Batam). *Jurnal Teknik Ibnu Sina JT-IBSI*, *1*(01).

Afrina, A., Veza, O., & Harnaranda, J. (2017). Implementasi Sistem Informasi Manajemen Pengolahan Data Periklanan pada Harian Umum Singgalang Padang Menggunakan Metode Pengolahan Data Terpusat (Centralized Data Processing Method). *JR: JURNAL RESPONSIVE Teknik Informatika*, *1*(1).