Analisis Risiko Teknologi Informasi Berbasis *Risk Management* Menggunakan Kerangka Kerja OCTAVE-S Pada Unit Pengelola Sistem Informasi Dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya

Via Aprilia Prabawati[1], Aditya Rachmadi[2] , Andi Reza Perdanakusuma[3]

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]vaprilea@gmail.com, [2]rachmadi.aditya@ub.ac.id, [3]andireza@gmail.com

Abstrak

Fakultas Ilmu Komputer Universitas Brawijaya merupakan salah satu fakultas yang telah menerapkan dan mengembangkan teknologi informasi di setiap aktivitas proses bisnisnya. Setiap aktivitas yang berhubungan dengan pengembangan sistem informasi dilakukan oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Meskipun dalam menjalankan tugas dan fungsinya Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer telah menggunakan sistem informasi yang lebih terkomputerisasi dan terintegrasi, namun mereka belum pernah melakukan pengukuran terhadap ancaman risiko maupun menerapkan manajemen risiko. Berdasarkan permasalahan tersebut maka diberikan solusi untuk melakukan proses pengukuran dan manajemen risiko dengan menggunakan kerangka kerja OCTAVE-S. Proses tersebut dilakukan dengan mengidentifikasi dan menganalisis ancaman risiko yang terdapat pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer yang kemudian akan digunakan untuk memberikan rekomendasi mitigasi sesuai dengan praktik keamanan yang dimiliki. Hasil dari penelitian ini didapatkan 3 area praktik keamanan yang memiliki status *stoplight* kuning dan 1 area praktik keamanan yang memiliki status *stoplight* merah. Keempat area praktik keamanan tersebut kemudian dipilih sebagai area mitigasi.

Kata kunci: *Analisis Risiko, Teknologi Informasi, Manajemen Risiko, OCTAVE-S, FMEA.*

Abstract

Fakultas Ilmu Komputer Universitas Brawijaya is one of the faculties that has implemented and developed information technology in every its business process activity. Each activity related to information system development is handled by the Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Although they have used a more computerized and integrated information system in conducting their duties and functions, they have never taken a risk assessment or implemented risk management. Based on the problem, solutions are provided to carry out the process of measuring and managing risk using the OCTAVE-S framework. The process is implemented by identifying and analyzing risk threats found in the Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer, which will then be used to provide mitigation recommendations in accordance with security practices. The results of this study found 3 security practice areas that have yellow stoplight status and 1 security practice area that have red stoplight status. The four areas of security practice were then selected as mitigation areas.

Keywords: *Risk Analysis, Information Technology, Risk Management, OCTAVE-S, FMEA*

1. PENDAHULUAN

Fakultas Ilmu Komputer Universitas Brawijaya merupakan salah satu fakultas yang telah menerapkan dan mengembangkan teknologi informasi di setiap aktivitas proses bisnisnya. Setiap aktivitas yang berhubungan dengan pengembangan sistem informasi dilakukan oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer.

Ketidakpastian dari risiko memungkinkan timbulnya akibat yang kurang menyenangkan, hal tersebut dapat berarti merugikan maupun membahayakan bagi penerima risiko. Berdasarkan risiko yang telah dijelaskan oleh jurnal Masing (2009), dengan menggunakan sistem dengan metode manajemen risiko teknologi informasi yang tepat dapat memberikan pengaruh yang positif bagi perusahaan diantaranya dapat mengetahui risiko dan kerentanan, serta dapat mengurangi biaya yang akan dikeluarkan apabila terjadi risiko.

Meskipun dalam menjalankan tugas dan fungsinya Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer telah menggunakan sistem informasi yang lebih terkomputerisasi dan terintegrasi, namun mereka belum pernah melakukan pengukuran terhadap ancaman risiko maupun menerapkan manajemen risiko. Maka, untuk meminimalisir kemungkinan terjadinya ancaman risiko pada Unit PSIK FILKOM perlu dilakukan pengukuran atau penilaian terhadap sistem yang mereka miliki. Sehingga Unit PSIK FILKOM akan dapat mengetahui besarnya ancaman risiko dan tingkat kerentanan dari setiap aset kritis yang dimiliki sehingga mereka dapat melakukan kontrol yang tepat dan sesuai untuk masing-masing aset kritis berdasarkan tingkat prioritas kekritisannya bagi organisasi tersebut serta memiliki ancaman risiko yang paling besar.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE-S) merupakan metode yang dapat digunakan untuk mengidentifikasi ancaman yang dapat menimbulkan risiko teknologi informasi. Metode OCTAVE-S akan menilai, menganalisis dan melakukan perencanaan strategis berbasis risiko keamanan dari berbagai perspektif organisasi (Alberts, 2005).

Pada penelitian ini akan dilakukan identifikasi dan analisis risiko teknologi informasi yang terdapat pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya dengan menggunakan kerangka kerja OCTAVE-S dan selanjutnya menggunakan metode FMEA untuk melakukan penilaian terhadap risiko yang telah diidentifikasi sebelumnya. Dari kedua analisis tersebut akan didapatkan hasil yang akan digunakan untuk membuat rekomendasi langkah mitigasi terhadap praktik keamanan yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer.

2. LANDASAN KEPUSTAKAAN

2.1 Teknologi Informasi

Teknologi informasi adalah segala bentuk teknologi yang diterapkan untuk memproses dan mengirimkan informasi dalam bentuk elektronis (Lucas, 2000). Sehingga dapat disimpulkan bahwa teknologi informasi merupakan teknologi yang digunakan untuk membantu mengolah dan memanipulasi data dengan berbagai cara untuk dapat menghasilkan informasi yang berkualitas. Dan diharapkan informasi tersebut dapat membantu dalam melakukan pengambilan keputusan.

2.2 Manajemen Risiko Teknologi Informasi

Teknologi informasi memiliki potensi risiko terhadap kemungkingkan kehilangan informasi dan memiliki serangkaian tindakan pemulihan yang tercakup dalam 6 kategori (Hughes, 2006), diantaranya:

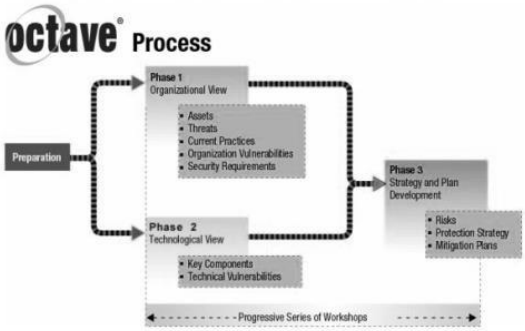
a. Keamanan
   Risiko terhadap keamanan informasi yang memiliki kemungkinan mengalami perubahan dan digunakan oleh pihak yang tidak berwenang.
b. Ketersediaan
   Risiko terhadap ketersediaan data yang tidak dapat diakses setelah terjadi kegagalan sistem yang diakibarkan oleh kesalahan manusia (*human error*).
c. Daya pulih
   Risiko terhadap informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup setelah terjadi kegagalan.
d. Performa
   Risiko terhadap informasi dimana informasi tidak tersedia saat diperlukan.

e. Daya skala
   Risiko yang terjadi akibat perkembangan bisnis dan bentuk arsitektur teknologi yang diterapkan tidak memungkinkan untuk menangani banyak aplikasi baru dan biaya bisnis secara efektif.
f. Ketaatan
   Risiko yang terjadi karena manajemen dan penggunaan informasi yang diberlakukan melanggar keperluan dari pihak pengatur.

Menurut Alberts, C dan Dorofee.A (2003), manajemen risiko merupakan proses berkelanjutan yang dilakukan untuk mengidentifikasi risiko dan menerapkan rencana untuk mengatasinya. Jordan dan Silcock dalam bukunya Beating The Risks, menjelaskan bahwa kemampuan manajemen risiko teknologi informasi yang efektif adalah kemampuan manajemen yang memenuhi kebutuhan bisnis.

2.3 OCTAVE-S

OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) merupakan sebuah teknik atau metode yang digunakan untuk melakukan penilaian dan perencanaan strategis keamanan informasi berbasis risiko. Kerangka kerja OCTAVE dapat digunakan untuk mengidentifikasi, menganalisa dan mengawasi proses pengelolaan risiko keamanan informasi.



Gambar 1. Proses OCTAVE
Sumber: OCTAVE

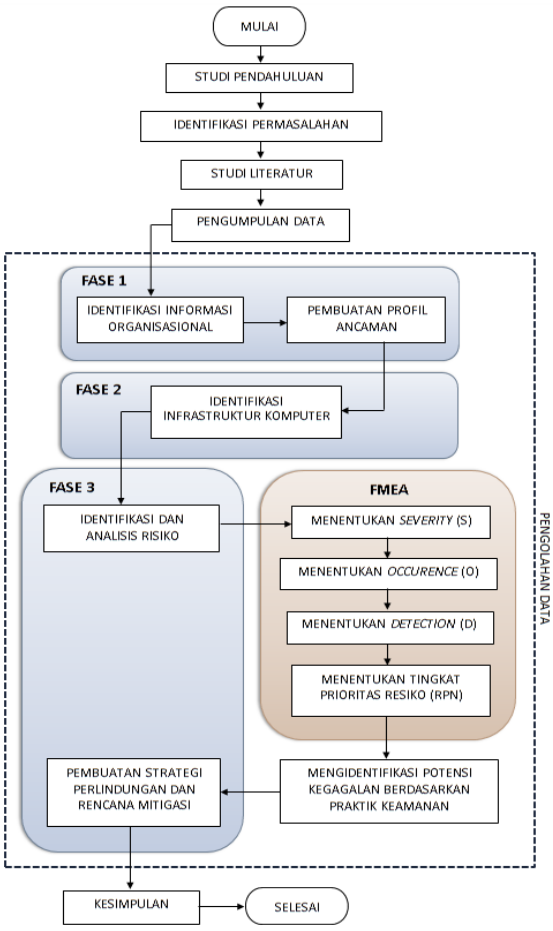
2.4 FMEA

Failure Mode and Effect Analysis (FMEA) merupakan suatu metode yang digunakan untuk mengidentifikasi dan menganalisa potensi kesalahan atau kegagalan di dalam sebuah sistem atau proses. Proses identifikasi kegagalan yang potensial dilakukan dengan cara pemberian nilai pada masing-masing mode kegagalan tersebut berdasarkan tingkat keparahan dampak (*severity*), tingkat probabilitas kejadian (*occurence*), dan tingkat kemampuan deteksi (*detection*). Selanjutnya ketiga hal tersebut akan dihitung untuk mencari nilai tingkat prioritas risiko (RPN). RPN dapat dihitung dengan menggunakan persamaan berikut ini:

RPN = *Severity* x *Occurence* x *Detection*

Dari hasil perhitungan tersebut maka akan diperoleh hasil yang digunakan untuk menentukan tingkat risiko.

3. METODOLOGI



Gambar 2. Kerangka Kerja Penelitian

3.1 Pengumpulan Data

Terdapat beberapa langkah yang dilakukan untuk melakukan pengumpulan dan pengolahan data diantaranya dengan menggunakan teknik wawancara dan observasi. Wawancara

dilakukan secara langsung kepada beberapa pihak yang dinilai memiliki kewenangan dan pengetahuan terkait dengan teknologi informasi yang diterapkan pada Unit PSIK FILKOM. Hal ini bertujuan agar narasumber dapat memberikan informasi yang valid dan sesuai serta relevan dengan cakupan wawancara itu sendiri.

Proses wawancara dilakukan dengan menggunakan kerangka kerja OCTAVE-S untuk mendapatkan data dan informasi yang akan digunakan untuk mendefinisikan profil ancaman. Selain itu juga akan digunakan untuk mengidentifikasi aset organisasi yang dianggap kritis serta melakukan evaluasi praktik keamanan organisasi yang ada saat ini. Kemudian dilakukan proses verifikasi untuk memastikan kebenaran data dan informasi tersebut, sehingga diperoleh data dan informasi yang dapat dipertanggung jawabkan.

3.2 Pengolahan Data

Pengolahan data dilakukan dengan menggunakan kerangka kerja OCTAVE-S dan metode FMEA. Kerangka kerja OCTAVE-S digunakan untuk mengidentifikasi dan menganalisis ancaman risiko teknologi informasi yang ada di dalam organisasi, sedangkan metode FMEA digunakan untuk mengidentifikasi dan menganalisa potensi kesalahan atau kegagalan di dalam sebuah sistem atau proses. Proses identifikasi kegagalan yang potensial dilakukan dengan cara pemberian nilai pada masing-masing mode kegagalan tersebut berdasarkan tingkat keparahan dampak (*severity*), tingkat probabilitas kejadian (*occurence*), dan tingkat kemampuan deteksi (*detection*) yang selanjutnya dihitung untuk mendapatkan nilai tingkat prioritas risiko (RPN).

Dari langkah-langkah tersebut maka akan didapatkan hasil yang kemudian digunakan untuk memberikan rekomendasi tindakan mitigasi pada organisasi dalam mengatasi potensi ancaman risiko yang dimiliki.

4. HASIL DAN PEMBAHASAN

4.1 Identifikasi Aset Kritis

Daftar aset organisasi yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya berdasarkan hasil wawancara langsung yang dilakukan pada Ketua Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya. Berikut merupakan tabel dari hasil identifikasi aset:

Tabel 1. Daftar Aset

No.	Kategori	Aset
1	Informasi, Sistem dan Aplikasi	FILKOM Apps
2		Infrastruktur Data dan Jaringan
3		Standar Operasional Prosedur (SOP)
4	Orang	Ketua Unit
5		Koordinator Divisi Pengembangan Sistem Informasi
6		Koordinator Divisi Infrastruktur Data dan Jaringan
7		Koordinator Divisi Multimedia dan Desain

4.2 Evaluasi Praktik Keamanan Organisasi

Evaluasi praktik keamanan dilakukan untuk mengetahui dan mendokumentasikan praktik yang diberlakukan oleh organisasi, kemudian dilakukan penilaian status *stoplight* untuk menentukan area praktik keamanan mana yang nantinya akan dimitigasi. Hasil dari evaluasi praktik keamanan organisasi dapat dilihat pada tabel 2.

Tabel 2. Evaluasi Praktik Keamanan

No	Praktik Keamanan	*Stoplight*
1	Kesadaran dan Pelatihan Keamanan	Hijau
2	Strategi Keamanan	Hijau
3	Manajemen Keamanan	Hijau
4	Peraturan dan Kebijakan Keamanan	Hijau
5	Manajemen Keamanan Kolaboratif	Hijau
6	Perencanaan *Contingency*/ Pemulihan Bencana	Hijau
7	Pengendalian Akses Fisik	Kuning
8	Pemantauan dan Audit Keamanan Fisik	Hijau
9	Manajemen Jaringan dan Sistem	Hijau
10	Pemantauan dan Audit Keamanan TI	Hijau
11	Autentikasi dan Otorisasi	Kuning

No	Praktik Keamanan	*Stoplight*
12	Manajemen Kerentanan	Kuning
13	Enkripsi	Hijau
14	Perancangan dan Arsitektur Keamanan	Hijau
15	Manajemen Insiden	Merah

Dari hasil evaluasi dan penilaian yang dilakukan pada area praktik keamanan organisasi didapatkan status *stoplight* dari masing-masing area. Terdapat 3 area yang mendapatkan status lampu Kuning atau *Yellow Stoplight*, artinya organisasi telah menjalankan sebagian dari area praktik kemanan tersebut atau hingga batas tertentu sehingga hanya membutuhkan sedikit perbaikan. Dan terdapat 1 area yang mendapatkan status lampu Merah atau *Red Stoplight*, artinya organisasi belum menjalankan praktik keamanan pada area tersebut sehingga dibutuhkan perbaikan yang signifikan. Area praktik keamanan yang berstatus *stoplight* kuning dan merah inilah yang nantinya akan dipilih sebagai area mitigasi.

4.3 Memilih Aset Kritis

Dari aset-aset yang telah teridentifikasi sebelumnya selanjutnya dipilih dua aset paling kritis yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer, yaitu FILKOM Apps dan Infrastruktur Data dan Jaringan. Kedua aset ini dipilih karena dinilai sebagai aset yang paling kritis bagi organisasi dan harus dilindungi dari adanya potensi ancaman risiko yang muncul.

Selanjutnya aktivitas identifikasi dan analisis risiko akan dilakukan pada kedua aset beserta dengan teknologi-teknologi lain yang terkait dengan aset tersebut seperti jalur akses, aktor hingga motif pelaku ancaman.

4.4 Identifikasi Ancaman

Proses identifikasi ancaman dilakukan dengan melaksanakan wawancara dengan ketua beserta staff IT dari Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Hasil identifikasi ancaman didapatkan dengan menentukan kejadian yang berpotensi atau memiliki probabilitas untuk menjadi ancaman risiko bagi aset kritis dari jalur akses jaringan, fisik, masalah sistem dan masalah lainnya baik itu berasal dari internal maupun eksternal organisasi serta baik yang dilakukan dengan sengaja maupun tidak sengaja. Hasil dari evaluasi praktik keamanan organisasi dapat dilihat pada tabel 3.

Tabel 3. Identifikasi Ancaman

Jalur Akses	Aktor	Motif	Tingkat Keyakinan
Jaringan	Internal	Tidak Sengaja	Sedang
		Sengaja	Sedang-Tinggi
	Eksternal	Tidak Sengaja	Rendah
		Sengaja	Sedang-Tinggi
Fisik	Internal	Tidak Sengaja	Rendah-Sedang
		Sengaja	Rendah
	Eksternal	Tidak Sengaja	Rendah-Sedang
		Sengaja	Rendah-Sedang
Masalah Sistem	Kerusakan *Software*		Sedang
	System Crashes		Sedang
	Kerusakan *Hardware*		Sedang
	Kode-kode Berbahaya		Sedang-Tinggi
Masalah Lainnya	Masalah *Power supply*		Rendah-Sedang
	Bencana Alam		Rendah-Sedang

4.5 Identifikasi Risiko

Tahap identifikasi risiko dilakukan pada kedua aset kritis untuk mengetahui risiko apa saja yang pernah terjadi dan apa yang menjadi penyebabnya. Pada tahapan ini dapat dilihat dari dua aspek utama yaitu kemungkinan ancaman serta kerentanan yang dimiliki oleh organisasi. Berikut ini merupakan hasil identifikasi risiko yang dilakukan pada aset kritis:

Tabel 4. Daftar Risiko

No.	Potensi Kegagalan	Penyebab
1.	Kerusakan data pada *database*	Human error
		Listrik mati
		Lupa *log out*
		Orang tidak bertanggung jawab
2.	Jaringan	Serangan hacker

No.	Potensi Kegagalan	Penyebab
	terganggu karena gangguan dari internal	Praktikum mata kuliah jaringan
3.	*Workstation* jaringan mengalami gangguan akibat *brute force attack*	Serangan hacker
4.	*Mouse* rusak	Orang yang tidak bertanggung jawab
5.	Jaringan terganggu karena penumpukan paket di *router*	Human error
6.	Layanan MySQL terputus	Listrik mati
		Kurangnya perawatan (maintenance)
7.	*Hardisk* penuh	Data dan file ganda atau duplikat
		Data dan file tidak penting
		Human error
8.	*Hardisk master* dan *slave* rusak	Human error
		Tidak dirawat dengan baik
9.	Komputer rusak karena *power supply*	Human error
		Listrik mati
10.	Ruang kerja bocor dan kebanjiran	Human error
		Bencana alam
11.	Jaringan internet melambat karena *router* dan *access point* mati akibat petir	Listrik mati
		Bencana alam

4.6 Mengidentifikasi Potensi Kegagalan Berdasarkan Praktik Keamanan

Analisis ini bertujuan untuk mengetahui keterkaitan antara kedua metode berdasarkan hasil identifikasi risiko dan praktik keamanan yang dimiliki oleh kerangka OCTAVE-S serta pengukuran dan penilaian tingkat prioritas risiko yang dimiliki oleh metode FMEA.

Tabel 5. Daftar Risiko dari Praktik Keamanan

No.	Area Praktik Keamanan	Potensi Kegagalan
1.	Pengendalian Akses Fisik	*Mouse* rusak
		Ruang kerja bocor dan kebanjiran
2.	Autentikasi dan Otorisasi	Kerusakan data pada *database*
		Jaringan terganggu karena penumpukan paket di *router*
		Jaringan terganggu karena gangguan dari internal
3.	Manajemen Kerentanan	*Hardisk* penuh
		Hardisk master dan *slave* rusak
		Kerusakan data pada *database*
		Jaringan terganggu karena gangguan dari internal
		Workstation jaringan mengalami gangguan akibat *brute force attack*
		Mouse rusak
		Komputer rusak karena *power supply*
		Layanan MySQL terputus
4.	Manajemen Insiden	*Mouse* rusak
		Komputer rusak karena *power supply*
		Ruang kerja bocor dan kebanjiran
		Jaringan internet melambat karena *router* dan *access point* mati akibat petir

4.7 Strategi Perlindungan dan Rencana Mitigasi

Berdasarkan hasil penilaian dan evaluasi praktik keamanan dengan menggunakan status *stoplight* yang telah dilakukan pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer, terdapat area yang memiliki status *stoplight* kuning dan merah. Area praktik keamanan yang berstatus kuning diantaranya Pengendalian Akses Fisik,

Autentikasi dan Otorisasi, dan Manajemen Kerentanan. Sedangkan area praktik keamanan yang berstatus merah adalah Manajemen Insiden. Area-area inilah yang kemudian akan dipilih untuk dilakukan mitigasi.

Setelah diketahui area praktik keamanan mana saja yang perlu dilakukan mitigasi oleh organisasi, maka kemudian dibuatlah rencana mitigasi risiko yang harus dibuat untuk area praktik keamanan tersebut. Rencana mitigasi risiko untuk area praktik keamanan tersebut adalah sebagai berikut:

a. Pengendalian Akses Fisik
   - Membuat rencana dan prosedur keamanan fasilitas secara resmi yang dapat diuji untuk menjaga tempat, bangunan dan setiap area yang terlarang untuk umum.
   - Membuat kebijakan dan prosedur untuk pengelolaan pengunjung aset fisik secara resmi.
   - Membuat kebijakan dan prosedur untuk melakukan akses kontrol terhadap akses fisik, baik pada media perangkat keras maupun lunak secara resmi.
   - Melakukan pengujian secara berkala terhadap dokumen-dokumen resmi yang berkaitan dengan praktik pengendalian akses fisik.
   - Mengatur ulang kantor atau ruang kerja untuk membatasi akses fisik ke sistem, komputer, atau perangkat lain oleh personel yang tidak sah.
   - Pertahankan layanan penjaga keamanan untuk melindungi tempat.
   - Memberikan atau menyediakan pelatihan kepada karyawan tentang pengendalian akses fisik untuk mengelola akses fisik ke gedung dan tempat, area kerja, perangkat keras TI, dan media perangkat lunak.

b. Autentikasi dan Otorisasi
   - Membuat dan menyediakan mekanisme formal untuk memastikan bahwa informasi penting yang dimiliki oleh organisasi tidak dapat diakses dan belum diubah atau dihancurkan dengan cara yang tidak sah.
   - Melakukan pengujian secara berkala terhadap mekanisme perlindungan informasi yang telah dibuat.

c. Manajemen Kerentanan
   - Membuat prosedur secara tertulis dan resmi serta dapat diuji untuk mengelola tingkat kerentanan.
   - Melakukan pengujian secara berkala terhadap prosedur kerentanan untuk memastikan kesesuaian dokumen dengan keadaan terkini dari organisasi.
   - Melakukan audit keamanan teknologi informasi untuk mengidentifikasi kelemahan keamanan di dalam infrastruktur komputasi.
   - Memberikan atau menyediakan pelatihan manajemen kerentanan kepada seluruh karyawan.

d. Manajemen Insiden
   - Membuat prosedur manajemen insiden secara resmi yang dapat diuji dan diverifikasi.
   - Melakukan pengujian secara berkala terhadap dokumen prosedur manajemen insiden untuk memastikan kesesuaian dokumen dengan keadaan terkini dari organisasi.
   - Memberikan atau menyediakan pelatihan manajemen insiden kepada seluruh karyawan.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah telah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Aset-aset kritis yang teridentifikasi pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer adalah FILKOM Apps dan Infrastruktur Data dan Jaringan.
2. Hasil dari analisis risiko yang dilakukan pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer dengan menggunakan kerangka kerja OCTAVE-S menunjukkan bahwa terdapat tiga area praktik keamanan yang memiliki status *stoplight* kuning diantaranya adalah Pengendalian Akses Fisik, Autentikasi dan Otorisasi, serta Manajemen Kerentanan. Sedangkan area praktik keamanan yang berstatus *stoplight* merah adalah Manajemen Insiden.
3. Setelah mengetahui hasil dari analisis risiko yang telah dilakukan pada Unit Pengelola Sistem Informasi dan

Kehumasan Fakultas Ilmu Komputer selanjutnya akan diberikan rekomendasi pada area praktik keamanan yang masih berstatus *stoplight* kuning dan merah sebagai langkah perbaikan.

DAFTAR PUSTAKA

Alberts, C. J. & Dorofee, A. 2002. *Managing Information Security Risks: The OCTAVE SM Approach.* Massachusetts: Addison Wesley.

Alberts, C. J., Dorofee, A. Stevens, J. & Woody, C. 2005. *OCTAVE-S Implementation Guide, Version 1.0.* Pittsburgh: Carneige Mellon Software Engineering Institute.

Hughes, G. 2006. Five Steps to IT Risk Management Best Practices. Risk Management, Vol 53, Issue 7. 34.

Lucas, H. 2000. *Information Technology for Management (7th ed.)*. New York: Irwin/McGraw-Hill.

Masing, E. 2009. Tehnical Support : Improving Performance and Reduing Costs With IT Risk Management. Risk Management Vol 56. 48-51.

Stamatis, D. H. 2003. *Failure Mode and Effect Analysis: FMEA from Theory to Execution. Second Edition.* Milwaukee: ASQ Quality Press Publications.