repository.ub.ac.id

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

SKRIPSI

Untuk memenuhi sebagian persyaratan memperoleh gelar
Sarjana Komputer

Disusun oleh:
Via Aprilia Prabawati
145150401111070

PROGRAM STUDI SISTEM INFORMASI
JURUSAN SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2018

UNIVERSITAS BRAWIJAYA

repository.ub.ac.id

PENGESAHAN

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

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Via Aprilia Prabawati
NIM: 145150401111070

Skripsi ini telah diuji dan dinyatakan lulus pada
28 Desember 2018
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
Aditya Rachmadi, S.ST., M.TI	Andi Reza Perdanakusuma , S.Kom., M.MT.
NIK: 2012018604211001	NIK: 2016078611281001

Mengetahui
Ketua Jurusan Sistem Informasi

Dr. Eng. Herman Tolle, S.T., M.T.
NIP: 19740823 200012 1 001

UNIVERSITAS BRAWIJAYA

repository.ub.ac.id

PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (sarjana) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, 17 Desember 2018

Via Aprilia Prabawati

NIM: 145150401111070

UNIVERSITAS BRAWIJAYA

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat, taufik dan hidayah-Nya sehingga laporan skripsi yang berjudul "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" ini dapat terselesaikan.

Penulis menyadari bahwa skripsi ini tidak akan berhasil tanpa bantuan dari beberapa pihak. Oleh karena itu, penulis ingin menyampaikan rasa hormat dan terima kasih kepada:

1. Bapak Aditya Rachmadi, S.ST., M.TI dan Bapak Andi Reza Perdanakusuma , S.Kom., M.MT. selaku Pembimbing skripsi yang telah dengan sabar membimbing, memberikan saran dan mengarahkan penulis sehingga dapat menyelesaikan skripsi ini,
2. Bapak Yusi Tyroni Mursityo, S.Kom., M.AB. selaku Ketua Program Studi Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya,
3. Bapak Ismiarta Aknuranda, S.T, M.Sc, Ph.D selaku Sekretaris Jurusan Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya,
4. Bapak Dr. Eng. Herman Tolle, S.T., M.T. selaku Ketua Jurusan Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya,
5. Kedua orang tua Bapak Geter Widodo dan Ibu Sunartin, serta seluruh keluarga besar atas segala nasihat, kasih sayang, perhatian dan kesabarannya di dalam membesarkan dan mendidik penulis, serta yang senantiasa tiada henti-hentinya memberikan doa, dukungan baik moriil maupun materiil, motivasi dan semangat demi terselesaikannya skripsi ini,
6. Bapak Denny Sagita Rusdianto, S.Kom, M.Kom beserta seluruh staf PSIK yang telah membantu penulis dalam proses penyelesaian skripsi ini,
7. Seluruh Civitas Akademika Fakultas Ilmu Komputer Universitas Brawijaya yang telah banyak memberi bantuan dan dukungan selama penulis menempuh studi di Informatika Universitas Brawijaya dan selama penyelesaian skripsi ini,
8. Teman-teman yang saling mendukung, memberikan doa, semangat dan membantu penulis baik secara langsung maupun tidak langsung yaitu Rhevitta, Erdiana, Clara, Hana, Jawara, Arul Septa, Rusdy, dan yang lainnya,
9. Teman-teman Kos Sumbersari 254 yang selalu memberikan dukungan, doa, dan semangat demi kelancaran skripsi penulis,
10. Diriku sendiri karena sudah mau berusaha, berdoa, dan bekerja keras untuk menyelesaikan skripsi ini dengan baik dan semaksimal mungkin. Terimakasih karena sudah bersedia menderita, bersusah payah, dan sering tidak tidur setiap revisian datang. Maaf sering membuatmu menangis dan kehilangan tenaga hingga nutrisimu

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

tidak tercukupi dengan baik. Maaf telah membuat tubuhmu lelah hingga ingin menyerah. Sekali lagi terimakasih banyak, kamu sudah bekerja keras dan memberikan yang terbaik. Terimakasih diriku. Aku mencintaimu.

11. BTS yang telah memberikan semangat dan motivasi bagi penulis untuk menyelesaikan skripsi ini dengan sebaik-baiknya. Terimakasih karena telah menciptakan lagu yang dapat menjadi penyemangat bagi siapa saja yang sedang jatuh dan membutuhkan teman. Lagu-lagu yang menunjukkan bahwa kamu tidak sendiri dan sebelum kamu mencintai orang lain, terlebih dahulu kamu harus mampu mencintai dirimu sendiri.
12. Seluruh pihak yang telah membantu kelancaran dalam pengerjaan skripsi yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih banyak kekurangan, sehingga saran dan kritik yang membangun sangat penulis harapkan. Semoga Allah SWT senantiasa membalas segala kebaikan dan jasa yang telah diberikan kepada penulis. Akhir kata penulis berharap skripsi ini dapat membawa manfaat bagi semua pihak yang menggunakannya.

Malang, 17 Desember 2018

Penulis

vaprilea@gmail.com

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

repository.ub.ac.id

ABSTRAK

Via Aprilia Prabawati, 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

Pembimbing: Aditya Rachmadi, S.ST., M.TI dan Andi Reza Perdanakusuma , S.Kom., M.MT.

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, FMEA.

UNIVERSITAS BRAWIJAYA

ABSTRACT

Via Aprilia Prabawati, Technology of Information Risk Analysis Based on Risk Management Using the OCTAVE-S Framework on Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya

Mentor: Aditya Rachmadi, S.ST., M.TI and Andi Reza Perdanakusuma , S.Kom., M.MT.

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, FMEA*

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

DAFTAR ISI

PENGESAHAN i
PERNYATAAN ORISINALITAS ii
KATA PENGANTAR iii
ABSTRAK v
ABSTRACT vi
DAFTAR ISI vii
DAFTAR TABEL x
DAFTAR GAMBAR xii
BAB 1 PENDAHULUAN 1
1.1 Latar belakang 1
1.2 Rumusan masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan 3
1.5 Manfaat 3
1.6 Sistematika Penulisan 4
BAB 2 TINJAUAN PUSTAKA 5
2.1 Kajian Pustaka 5
2.2 Profil Organisasi 6
2.3 Risiko 7
2.3.1 Pengertian Risiko 7
2.3.2 Jenis-jenis Risiko 8
2.3.3 Manajemen Risiko 9
2.4 Teknologi Informasi 11
2.4.1 Pengertian Teknologi Informasi 11
2.4.2 Pengertian Aset 12
2.4.3 Pengertian Aset Teknologi Informasi 12
2.4.4 Pengertian Sistem 14
2.4.5 Pengertian Informasi 14
2.4.6 Pengertian Sistem Informasi 14
2.4.7 Infrastruktur Teknologi Informasi 15
2.5 Risiko Teknologi Informasi 16

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

2.5.1 Manajemen Keamanan 16
2.5.2 Manajemen Keamanan Informasi 17
2.5.3 Aspek Keamanan Informasi 18
2.5.4 Kategori Risiko Teknologi Informasi 19
2.5.5 Manajemen Risiko Teknologi Informasi 19
2.6 OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*)-S 21
2.6.1 Fase 1 : Membangun Profil Ancaman Berbasis Aset 23
2.6.2 Fase 2 : Mengidentifikasi Kerentanan Infrastruktur 27
2.6.3 Fase 3 : Mengembangkan Strategi Perlindungan dan Rencana Keamanan 29
2.7 *Failure Mode and Effect Analysis* (FMEA) 35
2.7.1 Tujuan *Failure Mode and Effect Analysis* (FMEA) 36
2.7.2 Tahapan *Failure Mode and Effect Analysis* (FMEA) 37
BAB 3 METODOLOGI PENELITIAN 42
3.1 Identifikasi Permasalahan 44
3.2 Studi Literatur 44
3.3 Pengumpulan Data 44
3.3.1 Wawancara 44
3.3.2 Observasi 45
3.4 Pengolahan Data 45
3.4.1 Identifikasi Informasi Organisasional 45
3.4.2 Pembuatan Profil Ancaman 46
3.4.3 Identifikasi Infrastruktur Komputer 46
3.4.4 Identifikasi dan Analisis Risiko 47
3.4.5 Menentukan Tingkat Keparahan Dampak (*Severity*) 47
3.4.6 Menentukan Tingkat Probabilitas Kejadian (*Occurence*) 47
3.4.7 Menentukan Tingkat Kemampuan Deteksi (*Detection*) 47
3.4.8 Menentukan Tingkat Prioritas Risiko (RPN) 47
3.4.9 Mengidentifikasi Potensi Kegagalan Berdasarkan Praktik Keamanan 48
3.4.10 Pembuatan Strategi Perlindungan dan Rencana Mitigasi 48
3.5 Kesimpulan 49

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

BAB 4 HASIL 50
4.1 Persiapan Pengumpulan Data 50
4.1.1 Wawancara 50
4.2 Pengolahan Data dan Informasi 55
4.2.1 Fase 1: Membangun Profil Ancaman Berbasis Asets. 55
4.2.2 Fase 2: Mengidentifikasi Kerentanan Infrastruktur. 89
4.2.3 Fase 3: Mengembangkan Strategi Perlindungan dan Rencana Keamanan. 91
BAB 5 PEMBAHASAN 119
5.1 Pengendalian Akses Fisik 119
5.2 Autentikasi dan Otorisasi 120
5.3 Manajemen Kerentanan 120
5.4 Manajemen Insiden 121
BAB 6 PENUTUP 122
6.1 Kesimpulan 122
6.2 Saran 123
DAFTAR PUSTAKA 125
LAMPIRAN A DOKUMENTASI HASIL KERANGKA KERJA OCTAVE-S 128
LAMPIRAN B DOKUMENTASI HASIL PENILAIAN *FAILURE MODE AND EFFECT ANALYSIS* (FMEA) 176
LAMPIRAN C HASIL WAWANCARA 190
LAMPIRAN D DOKUMENTASI ASET 191

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

DAFTAR TABEL

Tabel 2.1 Kajian Pustaka 6
Tabel 2.2 Perbedaan OCTAVE dengan Pendekatan lainnya 22
Tabel 2.3 Fase Membangun Profil Ancaman Berbasis Aset 23
Tabel 2.4 Fase Mengidentifikasi Kerentanan Infrastruktur 27
Tabel 2.5 Fase Mengembangkan Strategi dan Rencana Keamanan 29
Tabel 2.6 OCTAVE-S *Outputs* 34
Tabel 4.1 Ketentuan Wawancara 50
Tabel 4.2 Profil Narasumber 51
Tabel 4.3 Jumlah dan Tujuan Wawancara 52
Tabel 4.4 Daftar Pertanyaan Wawancara 53
Tabel 4.5 Kriteria Evaluasi Dampak 55
Tabel 4.6 Aset Organisasi (Informasi, Sistem dan Aplikasi) 57
Tabel 4.7 Aset Organisasi (Orang) 58
Tabel 4.8 Kesadaran dan Pelatihan Keamanan 59
Tabel 4.9 Strategi Keamanan 61
Tabel 4.10 Manajemen Keamanan 61
Tabel 4.11 Peraturan dan Kebijakan Keamanan 63
Tabel 4.12 Manajemen Keamanan Kolaboratif 64
Tabel 4.13 Perencanaan Contingency atau Pemulihan Bencana 65
Tabel 4.14 Pengendalian Akses Fisik 66
Tabel 4.15 Pemantauan dan Audit Keamanan Fisik 67
Tabel 4.16 Manajemen Jaringan dan Sistem 67
Tabel 4.17 Pemantauan dan Audit Keamanan TI 69
Tabel 4.18 Autentikasi dan Otorisasi 70
Tabel 4.19 Manajemen Kerentanan 70
Tabel 4.20 Enkripsi 71
Tabel 4.21 Perancangan dan Arsitektur Keamanan 72
Tabel 4.22 Manajemen Insiden 73
Tabel 4.23 Status *Stoplight* 73
Tabel 4.24 Aset Kritis 75
Tabel 4.25 Kebutuhan Keamanan untuk Aset Kritis 76

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Tabel 4.26 Pelaku Ancaman pada FILKOM Apps 77
Tabel 4.27 Pelaku Ancaman pada Infrastruktur Data dan Jaringan 79
Tabel 4.28 Tingkat Keyakinan Motif pada FILKOM Apps 81
Tabel 4.29 Tingkat Keyakinan Motif pada Infrastruktur Data dan Jaringan 82
Tabel 4.30 Frekuensi Kejadian pada FILKOM Apps 83
Tabel 4.31 Frekuensi Kejadian pada Infrastruktur Data dan Jaringan 84
Tabel 4.32 Potensi Ancaman pada FILKOM Apps 85
Tabel 4.33 Potensi Ancaman pada Infrastruktur Data dan Jaringan 87
Tabel 4.34 Kelas Komponen 89
Tabel 4.35 Evaluasi Dampak Ancaman 91
Tabel 4.36 Evaluasi Probabilitas 92
Tabel 4.37 Probabilitas Ancaman 93
Tabel 4.38 Tingkat Keparahan Dampak (*Severity*) 102
Tabel 4.39 Tingkat Probabilitas Kejadian (*Occurence*) 104
Tabel 4.40 Evaluasi Pengendalian 106
Tabel 4.41 Tingkat Kemampuan Deteksi (*Detection*) 107
Tabel 4.42 Hasil Perhitungan Tingkat Prioritas Risiko (RPN) 109
Tabel 4.43 Potensi Kegagalan Berdasarkan Praktik Keamanan 111
Tabel 4.44 Strategi Perlindungan Aspek Keamanan 114

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

DAFTAR GAMBAR

Gambar 2.1 Proses Manajemen Risiko 10
Gambar 2.2 Hubungan Antara Tiga Aspek OCTAVE 22
Gambar 2.3 Proses OCTAVE 23
Gambar 3.1 Kerangka Kerja Penelitian 43

BAB 1 PENDAHULUAN

1.1 Latar belakang

Perkembangan teknologi informasi telah menjadi hal yang sangat penting dalam kehidupan masyarakat. Bahkan saat ini keberadaan teknologi informasi sudah menjadi suatu kebutuhan. Dampak dari penerapan teknologi informasi tersebut dapat dilihat di segala bagian termasuk pada institusi pendidikan. Sebagian besar institusi pendidikan bersaing dalam menerapkan teknologi informasi untuk dapat meningkatkan daya saing dan nilai tambah. Penerapan teknologi informasi yang baik memiliki peran yang penting dalam mendukung dan meningkatkan kegiatan akademik maupun proses bisnis yang dimiliki oleh organisasi. Untuk dapat memenuhi kebutuhan informasi yang diharapkan oleh pengguna, maka setiap komponen teknologi yang terdapat di dalam sistem harus saling terintegrasi.

Menurut jurnal yang disusun oleh Anjar Priandoyo (2006), pengukuran atau *assessment* adalah hal mutlak yang harus dilakukan untuk meningkatkan kualitas. Dengan adanya pengukuran maka perusahaan akan dapat mengetahui kelemahan dan kekurangan yang dimiliki untuk kemudian dapat dibandingkan dengan perusahaan lain sehingga akan menghasilkan solusi untuk mengingkatkan keuntungan perusahaan. Memahami dimensi risiko teknologi informasi dan mengetahui cara yang tepat untuk mengelolanya merupakan hal yang penting agar bisa mendapatkan keuntungan yang kompetitif dan salah satu cara yang dapat dilakukan adalah dengan melakukan pengukuran terhadap risiko yang dihadapi dalam penerapan teknologi informasi.

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. Penerapan teknologi informasi yang dilakukan tersebut salah satunya diwujudkan dengan adanya aplikasi FILKOM Apps. FILKOM Apps merupakan sebuah sistem informasi yang terintegrasi dengan proses bisnis yang berjalan pada Fakultas Ilmu Komputer. Hal tersebut bertujuan untuk mengurangi manualisasi yang dilakukan oleh civitas akademik, serta memudahkan dalam pengelolaan data dan informasi.

Ketidakpastian dari risiko memungkinkan timbulnya akibat yang kurang menyenangkan, hal tersebut dapat berarti merugikan maupun membahayakan bagi penerima risiko. Risiko juga didefinisikan oleh Martono dan Agus Harjito (2012) sebagai penyimpangan hasil yang diperoleh dari rencana hasil yang diharapkan. Sebuah risiko terjadi karena adanya penyebab dan memiliki konsekuensi yang harus diterima. 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.

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Dalam melakukan manajemen risiko, Robert Charette mengklasifikasikan strategi yang digunakan kedalam dua jenis yaitu, strategi penanganan risiko secara reaktif dan proaktif. Pada penanganan risiko secara reaktif, melakukan tindakan manajemen risiko setelah ancaman risiko tersebut terjadi. Selanjutnya akan diambil tindakan untuk mengurangi dampak negatif yang dihasilkan dari risiko tersebut agar tidak mengganggu jalannya proses bisnis yang dimiliki oleh organisasi atau perusahaan. Sedangkan pada penanganan risiko secara proaktif, aktivitas manajemen risiko telah dilakukan jauh sebelum ancaman risiko terjadi. Penanganan proaktif bertujuan untuk membuat sebuah perencanaan untuk menghindari kemungkinan terjadinya risiko beserta dampak yang akan dihasilkan. Menghindari risiko dapat dilakukan dengan mengidentifikasi risiko potensial serta probabilitas terjadinya risiko tersebut baik di masa yang lalu maupun di masa yang akan datang. Dengan ini maka organisasi atau perusahaan akan dapat mengembangkan rencana yang mudah untuk memberikan respon yang tepat, efektif dan terkontrol.

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. Kemudian setelah dilakukan pengukuran atau penilaian, 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. OCTAVE-S memanfaatkan kemampuan organisasi untuk memahami dan menilai pengetahuan dari beberapa pihak mengenai praktek keamanan yang terjadi di organisasi serta melihat kondisi praktek keamanan yang telah berjalan (Alberts, 2005).

Berdasarkan penjelasan tersebut maka 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. Diharapkan dengan dilakukannya analisis tersebut dapat memberikan hasil untuk kemudian diberikan kepada pihak Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya sebagai dasar dari rangkaian aktivitas manajemen risiko. Oleh karena itu, maka dilakukan penelitian dengan judul "Analisis Risiko Teknologi Informasi Berbasis *Risk Management* Menggunakan Kerangka Kerja OCTAVE-S pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Brawijaya", dimana penelitian ini ditujukan untuk melakukan analisis risiko pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya dengan menggunakan kerangka kerja OCTAVE-S.

1.2 Rumusan masalah

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah yang diambil dalam penelitian ini adalah sebagai berikut:

1. Bagaimana hasil identifikasi aset kritis dengan mengunakan kerangka kerja OCTAVE-S pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya?
2. Bagaimana hasil analisis risiko yang berpengaruh terhadap praktik keamanan pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya?
3. Bagaimana usulan mitigasi terhadap praktik keamanan informasi yang diberikan pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya?

1.3 Batasan Masalah

Agar penelitian ini dapat mencapai sasaran dan tujuan yang diharapkan, maka permasalahan ini terbatas pada:

1. Penelitian dilakukan pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya.
2. Penelitian dilakukan dengan menggunakan kerangka kerja OCTAVE-S.

1.4 Tujuan

Tujuan dari penelitian yang dilakukan dalam bentuk penulisan skripsi antara lain sebagai berikut:

1. Melakukan identifikasi identifikasi aset kritis dengan mengunakan kerangka kerja OCTAVE-S pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya
2. Mengetahui hasil analisis risiko yang berpengaruh terhadap praktik keamanan pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya.
3. Memberikan usulan mitigasi terhadap praktik keamanan informasi yang diberikan pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya.

1.5 Manfaat

Manfaat yang didapatkan dari penelitian tentang analisis risiko yang telah dilakukan adalah sebagai berikut:

1. Memberikan penilaian terhadap tingkat risiko teknologi informasi yang ada pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK)

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Fakultas Ilmu Komputer Universitas Brawijaya sesuai dengan kriteria OCTAVE-S.

2. Hasil dari penelitian dapat digunakan sebagai dasar rekomendasi untuk melakukan aktivitas manajemen risiko selanjutnya oleh pihak Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya.
3. Menambah wawasan serta pengetahuan terkait dengan pengelolaan risiko yang ada pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya.

1.6 Sistematika Penulisan

Sistematika penulisan pada skripsi ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Berisi tentang latar belakang penelitian, rumusan masalah, tujuan, manfaat, batasan masalah, serta sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai dasar teori yang digunakan dalam mendukung topik penelitian. Pada bab ini juga memuat kajian pustaka yang terdapat referensi skripsi ataupun jurnal dengan penelitian yang hampir sama atau relevan.

BAB 3 METODOLOGI PENELITIAN

Pada bab ini menjelaskan langkah – langkah yang di tempuh atau metode penelitian yang digunakan dalam melakukan penelitian ini. Metode tersebut memuat dalam pengambilan data, dalam pengolahan data serta analisis dan hasil yang atau bahkan rekomendasi yang diberikan dari hasil penelitian ini.

BAB 4 HASIL

Pada bab ini memuat tentang penjelasan hasil temuan yang didapat setelah melakukan pengumpulan data berupa wawancara, observasi, dan kuisoner

BAB 5 PEMBAHASAN

Pada bab ini menjelaskan tentang hasil dari observasi wawancara dan kuisoner yang nantinya berupa temuan yang nantinya di analisis dan diberikan rekomendasi sesuai dengan hasil temuan yang ada.

BAB 6 PENUTUP

Pada bab ini memuat hasil kesimpulan dari penelitian yang sudah di lakukan serta saran yang di berikan untuk dijadikan referensi atau perbaikan pada penelitian selanjutnya.

BAB 2 TINJAUAN PUSTAKA

2.1 Kajian Pustaka

Kajian pustaka berisi penjelasan mengenai penelitian yang telah dilakukan sebelumnya serta dasar teori atau landasan yang digunakan sebagai acuan pengerjaan tugas akhir ini. Penelitian yang dijadikan acuan dalam mengerjakan penelitian ini diantara lain adalah penelitian yang dilakukan oleh Kevin, dkk mengenai pengukuran risiko teknologi informasi dengan pendekatan OCTAVE-S pada PT. Mandala Multifinance, Tbk.

Penelitian kedua yang digunakan adalah penelitian yang dilakukan oleh Tommy Sanjaya, dkk tentang pengukuran risiko teknologi informasi pada Kementerian Komunikasi Dan Informatika dengan metode OCTAVE-S. Serta penelitian ketiga yang digunakan adalah penelitian yang dilakukan oleh Asmaya Rhasyid, dkk mengenai pengukuran risiko teknologi informasi pada Rumah Sakit Bhakti Yudha dengan menggunakan metode OCTAVE-S. Ketiga penelitian diatas tersebut menggunakan pendekatan kerangka kerja yang sama yaitu OCTAVE-S untuk mengidentifikasi aset teknologi informasi beserta ancaman risiko yang ada pada aset tersebut. Selain itu OCTAVE-S juga digunakan untuk menganalisis kebutuhan praktik keamanan yang sesuai untuk organisasi tersebut.

Penelitian selanjutnya yang digunakan adalah penelitian yang dilakukan oleh Stephanus mengenai penerapan kerangka kerja OCTAVE-S dan kontrol ISO 27001 dalam manajemen risiko sistem informasi. Pada penelitian tersebut digunakan kerangka kerja OCTAVE-S untuk mengidentifikasi ancaman risiko dan menganalisis kebutuhan praktik keamanan informasi. Sedangkan kontrol ISO 27001 digunakan sebagai kontrol mitigasi yang tepat dan sesuai untuk digunakan.

Penelitian berikutnya dilakukan oleh Rudi Harahap mengenai pengukuran risiko teknologi informasi dengan menggunakan metode OCTAVE-S. Pada penelitian tersebut dilakukan identifikasi risiko teknologi informasi pada perusahaan TIS. Ltd, serta membuat rekomendasi langkah penanganan risiko yang sesuai untuk mengatasi risiko yang terjadi. OCTAVE-S dipilih karena telah banyak risiko yang terjadi pada perusahaan tersebut namun belum ada pengukuran atau penilaian risiko yang dilakukan. Selain itu belum adanya alat yang digunakan dalam melakukan menjadi alasan penggunaan OCTAVE-S.

Penelitian selanjutnya dilakukan oleh Bambang Gunawan mengenai penilaian risiko teknologi informasi menggunakan pendekatan OCTAVE-S. Pada penelitian tersebut dilakukan identifikasi terhadap risiko teknologi informasi yang ada pada perusahaan GST. Ltd. Setelah melakukan identifikasi risiko kemudian memberikan rekomendasi tindakan untuk mengatasi masalah yang muncul. GST. Ltd menyadari bahwa semakin banyaknya kompetitor mengharuskan mereka untuk terus berinovasi terutama peningkatan dalam hal penanganan risiko.

Tabel 2.1 Kajian Pustaka

No.	Judul	Obyek	Metode	Hasil
1.	Pengukuran Risiko Teknologi Informasi Dengan Pendekatan OCTAVE-S Pada PT. Mandala Multifinance, Tbk	Perusahaan Pembiayaan (Bank Pinjaman Kredit)	OCTAVE-S	Menghasilkan daftar aset kritis, daftar risiko dan kebutuhan praktik keamanan informasi.
2.	Pengukuran Risiko Teknologi Informasi Pada Kementerian Komunikasi Dan Informatika Dengan Metode OCTAVE-S	Kementrian	OCTAVE-S	Menghasilkan daftar aset kritis, daftar risiko dan kebutuhan praktik keamanan informasi.
3.	Pengukuran Risiko Teknologi Informasi Pada Rumah Sakit Bhakti Yudha Dengan Menggunakan Metode OCTAVE-S	Rumah Sakit	OCTAVE-S	Menghasilkan daftar aset kritis, daftar risiko dan kebutuhan praktik keamanan informasi.
4.	*Implementation OCTAVE-S and ISO 27001 Controls in Risk Management Information Systems*	Perusahaan	OCTAVE-S dan ISO 27001	Menghasilkan daftar risiko, kebutuhan praktik keamanan informasi dan kontrol mitigasi risiko.
5.	*Information Technology Risk Measurement: OCTAVE-S Method*	Perusahaan	OCTAVE-S	Didapatkan tiga bidang penting, seperti pelatihan kesadaran dan keamanan, strategi keamanan, manajemen keamanan, dan pemulihan bencana.
6.	*Information Technology Risk Assessment: OCTAVE-S Approach*	Perusahaan Konstruksi	OCTAVE-S	Menghasilkan daftar aset kritis, daftar risiko dan rekomendasi tindakan yang akan dilakukan jika terjadi risiko.

2.2 Profil Organisasi

Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer merupakan suatu unit yang mengelola sistem informasi dan infrastruktur teknologi informasi yang berada di tingkat Fakultas. PSIK dipimpin

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

oleh seorang Koordinator yang diangkat dan bertanggung jawab kepada Dekan. Dalam menjalankan tugas dan fungsinya, PSIK dibagi menjadi beberapa bagian antara lain, bagian publikasi dan kehumasan; pendataan dan sistem informasi; infrastruktur; serta penanganan keluhan.

Sebagai unit yang bertugas mengelola sistem informasi dan infrastruktur teknologi informasi yang ada di Fakultas Ilmu Komputer, PSIK FILKOM berinovasi dengan membuat suatu sistem informasi yang terintegrasi dengan proses bisnis yang berjalan pada Fakultas Ilmu Komputer bernama FILKOM Apps. Hal tersebut bertujuan untuk mengurangi manualisasi yang dilakukan oleh civitas akademik, serta memudahkan dalam pengelolaan data dan informasi.

FILKOM Apps mengintegrasikan seluruh bagian yang ada di Fakultas Ilmu Komputer seperti bagian akademik, kemahasiswaan, kepegawaian, keuangan, sekretariat, hingga laboratorium. Sistem yang dimiliki oleh FILKOM Apps membantu mengatur aktivitas yang dimiliki oleh bagian-bagian tersebut seperti pengelolaan jadwal kuliah, aktivitas belajar dan mengajar, kegiatan mahasiswa, hingga peminjaman fasilitas yang dimiliki oleh Fakultas Ilmu Komputer. Oleh karena itu, kehadiran FILKOM Apps dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik Fakultas Ilmu Komputer.

2.3 Risiko

2.3.1 Pengertian Risiko

Risiko merupakan suatu peristiwa atau keadaan yang tidak pasti. Abas Salim mendefinisikan risiko sebagai sebuah ketidakpastian (*uncertainty*) yang mungkin akan menghasilkan adanya kerugian (*loss*). Menurut AS/NZS 4360, risiko adalah kemungkinan terjadinya sesuatu yang akan berdampak pada tujuan. Hal tersebut diukur dari segi konsekuensi dan kemungkinan.

Ketidakpastian dari risiko memungkinkan timbulnya akibat yang kurang menyenangkan, hal tersebut dapat berarti merugikan maupun membahayakan bagi penerima risiko. Risiko juga didefinisikan oleh Martono dan Agus Harjito (2012) sebagai penyimpangan hasil yang diperoleh dari rencana hasil yang diharapkan. Sebuah risiko terjadi karena adanya penyebab dan memiliki konsekuensi yang harus diterima.

Mamduh M. Hanafi menerangkan bahwa risiko dibagi menjadi beberapa macam. Pengelompokan risiko ini dinilai sebagai salah satu cara untuk mengetahui tipe-tipe risiko. Risiko dikelompokkan ke dalam dua tipe yaitu, risiko murni dan risiko spekulatif; risiko subjektif dan objektif; serta risiko dinamis dan statis.

a. Risiko murni (*pure risk*)
   Risiko murni memiliki arti risiko yang tidak disengaja. Risiko murni memiliki kemungkinan untuk adanya kerugian namun tidak ada kemungkinan untuk adanya keuntungan. Contoh risiko jenis ini antara lain risiko kecelakaan, kebakaran, bencana alam dan lain sebagainya.
b. Risiko spekulatif

Risiko spekulatif atau risiko yang disengaja adalah risiko yang sengaja ditimbulkan oleh pihak yang bersangkutan. Risiko spekulatif memiliki kemungkinan adanya kerugian serta adanya keuntungan. Contoh dari risiko spekulatif adalah utang-piutang dan usaha bisnis. Di dalam melakukan kegiatan bisnis, pelaku bisnis akan selalu mengharapkan keuntungan meskipun adanya potensi kerugian.

c. Risiko subjektif
Risiko subjektif merupakan risiko yang berkaitan dengan cara pandang seseorang tehadap risiko. Pada risiko jenis ini kondisi mental seseorang akan mempengaruhi dalam pengambilan kesimpulan terhadap risiko tersebut. Masing-masing orang akan memiliki pandangan yang berbeda terhadap risiko yang muncul.

d. Risiko objektif
Risiko objektif merupakan risiko yang didasarkan kepada observasi dengan parameter yang objektif. Risiko jenis ini dapat diukur dengan relatif mudah dengan menggunakan distribusi probabilita, distribusi normal dan distribusi lainnya.

e. Risiko dinamis
Risiko dinamis adalah risiko yang muncul akibat perubahan dari kondisi tertentu. Sebagai contoh, adanya perubahan teknologi dan perubahan kondisi masyarakat. Perubahan-perubahan tersebut berpotensi untuk menimbulkan jenis risiko baru.

f. Risiko statis
Risiko statis adalah risiko muncul dari akibat kondisi keseimbangan tertentu. Sebagai contoh, risiko terkena banjir merupakan risiko yang muncul akibat keadaan alam tertentu. Karakteristik dari risiko statis tidak berubah dari waktu ke waktu.

2.3.2 Jenis-jenis Risiko

Menurut Gondodiyoto (2009), risiko dapat dibedakan dalam beberapa jenis, yaitu:

a. Risiko Bisnis (*Business Risks*)
Risiko bisnis merupakan risiko yang dapat disebabkan oleh faktor-faktor internal (permasalahan kepegawaian, mesin, dan sebagainya) maupun disebabkan oleh faktor-faktor eksternal (perubahan kondisi perekonomian, perubahan tingkat kurs yang tiba-tiba, dan sebagainya) yang memungkinakan tidak tercapainya tujuan organisasi.

b. Risiko Bawaan (*Inherent Risks*)
Risiko bawaan merupakan risiko yang muncul akibat potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan apabila tidak terdapat pengendalian internal. Sebagai contoh pada kegiatan kampus, jika tidak ada absensi maka akan banyak mahasiswa yang tidak hadir.

c. Risiko Pengendalian (*Control Risks*)
Risiko pengendalian merupakan risiko yang tetap muncul meskipun sudah dilakukan pengendalian. Sebagai contoh, meskipun sudah ada absensi

namun tetap saja terdapat beberapa mahasiswa yang tidak hadir dengan melakukan titip absen.

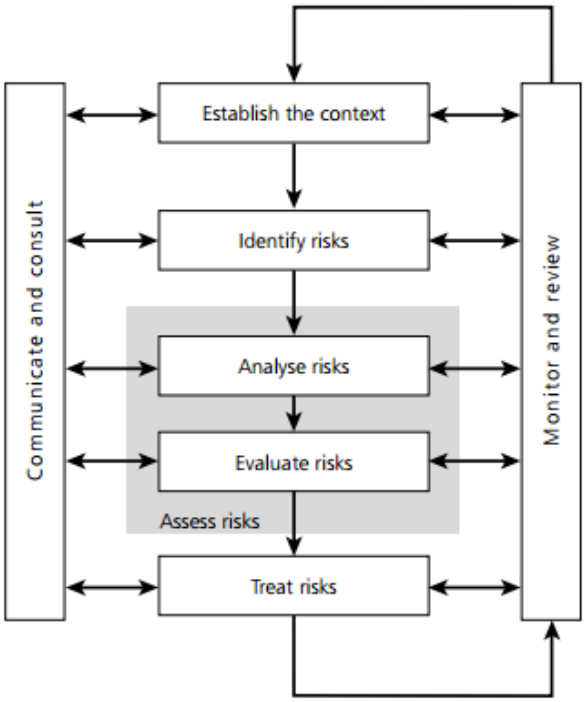
d. Risiko Deteksi (*Detection Risks*)
   Risiko deteksi merupakan risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya permasalahan yang cukup atau adanya kemungkinan *fraud* (penipuan).
e. Risiko Audit (*Audit Risks*)
   Risiko audit merupakan risiko dimana hasil pemeriksaan yang dilakukan auditor ternyata belum mencerminkan keadaan sesungguhnya.

2.3.3 Manajemen Risiko

Manajemen risiko adalah suatu proses yang dilakukan oleh dewan direksi, manajemen dan personil lainnya. Proses tersebut diterapkan dalam penetapan strategi dan seluruh perusahaan yang dirancang untuk mengidentifikasi kejadian potensial yang dapat mempengaruhi organisasi. Proses mengelola risiko berada dalam *risk appetite* untuk memberikan keyakinan yang memadai mengenai pencapaian tujuan organisasi (COSO).

Sedangkan menurut AS/NZS 4360 Risk Management Standard 2004, manajemen risiko merupakan budaya, proses, atau struktur yang diarahkan untuk mengelola peluang maupun ancaman potensial sambil mengelola efek samping yang muncul secara efektif. Manajemen risiko juga didefinisikan sebagai sebuah proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternatif penanganan risiko serta memonitor dan mengendalikan penanganan risiko (Djohanputro, 2008).

Manajemen risiko dapat diterapkan di berbagai tingkatan dalam sebuah organisasi. Penerapannya dapat dilakukan pada tingkat strategis dan tingkat operasional. Manajemen risiko dapat diterapkan pada proyek-proyek tertentu, untuk membantu membuat keputusan atau untuk mengelola area risiko yang diakui secara spesifik. Manajemen risiko memiliki serangkaian proses seperti pada bagan dibawah ini:



Gambar 2.1 Proses Manajemen Risiko

(Sumber: AS/NZS 4360:1999)

a. *Establish the context* (menetapkan konteks)
   Menetapkan konteks organisasi, manajemen risiko dan strategi apa yang akan digunakan untuk mengatasi risiko.
b. *Identify risks* (mengidentifikasi risiko)
   Mengidentifikasi penyebab munculnya risiko untuk dijadikan dasar analisis selanjutnya.
c. *Analyze risks* (menganalisa risiko)
   Melakukan analisa terhadap risiko-risiko yang ada dengan melakukan penilaian risiko.
d. *Evaluate risks* (melakukan evaluasi risiko)
   Membandingkan nilai risiko yang didapatkan dengan matriks risiko yang telah dibuat dan ditetapkan sebelumnya. Penilaian risiko biasanya dilakukan dengan menentukan level risiko tersebut (*low, medium,* dan *high*). Hal tersebut nantinya akan diguanakan untuk menentukan prioritas dalam penanganan risiko.
   Selain akan ditentukan apakah risiko tersebut dapat diterima (*acceptable*) atau tidak (*unacceptable*)
e. *Treat risks* (pengendalian risiko)
   Menerima serta melakukan pengendalian dan kontrol terhadap risiko dengan prioritas rendah (*low-priority*) atau risiko yang sudah dapat diterima (*acceptable*). Selain itu juga melakukan pengendalian dan kontrol terhadap risiko yang memiliki nilai tinggi agar menjadi rendah sehingga dapat diterima.

f. *Communicate and consult* (komunikasi dan konsultasi)
   Berkomunikasi dan berkonsultasi dengan pemangku kepentingan baik internal dan eksternal mengenai masing-masing tahapan proses manajemen risiko dan mengenai proses secara keseluruhan.
g. *Monitor and review* (pemantauan dan peninjauan ulang)
   Melakukan pemantauan dan peninjauan ulang terhadap kinerja sistem manajemen risiko yang telah dibuat. Hal tersebut berfungsi untuk mengantisipasi adanya perubahan-perubahan baik pada metode maupun kontrol sehingga akan memengaruhi nilai risiko.

Masing-masing elemen pada manajemen risiko tersebut harus dilakukan secara berurutan serta terus dilakukan peninjauan ulang agar dapat dilakukan perbaikan secara berkelanjutan.

Pada dasarnya manajemen risiko bertujuan untuk mengelola risiko tersebut sehingga akan didapatkan hasil yang optimal. Dalam melakukan pengelolaan risiko terdapat beberapa cara yang dapat digunakan diantaranya:

1. Menghindari risiko (*risk avoidance*)
   Menghindari risiko dapat dilakukan dengan memutuskan untuk tidak melaksanakan atau melanjutkan aktivitas yang berpotensi untuk mendatangkan risiko.
2. Berbagi risiko (*risk sharing/risk transfer*)
   Berbagi risiko dapat dilakukan dengan mengurangi kemungkinan munculnya risiko atau dampak risiko. Tindakan mengurangi risiko tersebut dapat dilakukan dengan memindahkan risiko kepada pihak lain.
3. Mitigasi (*mitigation*)
   Mitigasi risiko merupakan tindakan untuk mengurangi kemungkinan timbulnya risiko atau mengurangi dampak risiko yang dihasilkan dari risiko yang muncul.
4. Menerima risiko (*risk acceptance*)
   Menerima risiko berarti tidak melakukan tindakan apapun terhadap risiko yang terjadi serta dampak yang dihasilkan oleh risiko tersebut. Dalam hal ini organisasi benar-benar menerima risiko sepenuhnya.

2.4 Teknologi Informasi

Teknologi informasi (IT) mempunyai peran penting dalam memenuhi kebutuhan manusia terhadap keberadaan dan ketersediaan informasi. Teknologi informasi dapat membantu manusia dalam mengolah, mengkomunikasikan serta menyebarkan informasi.

2.4.1 Pengertian Teknologi Informasi

Teknologi informasi adalah segala bentuk teknologi yang diterapkan untuk memproses dan mengirimkan informasi dalam bentuk elektronis (Lucas, 2000). Namun teknologi informasi tidak hanya terbatas kepada teknologi komputer (*software & hardware*) yang digunakan untuk memproses atau menyimpan informasi, melainkan juga mencakup teknologi komunikasi untuk mengirimkan

informasi (Martin, 1999). Jadi 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.

2.4.2 Pengertian Aset

Aset merupakan segala sesuatu baik yang tangible maupun intangible, memiliki nilai ekonomis (*economic value*) dan masa ekonomis (*economic life*) untuk mendukung organisasi atau perusahaan dalam memberikan layanan (*services*) (Ouertani, 2008). Aset juga dapat diartikan sebagai barang atau apapun yang memiliki nilai ekonomi (*economic value*), nilai komersial (*commercial value*), atau nilai tukar (*exchange value*) yang dimiliki oleh suatu instansi, organisasi, badan usaha, inidividu atau bahkan perorangan (Hidayat, 2011).

Sedangkan Munawir menjelaskan jika aset merupakan sarana atau sumber daya ekonomik yang dimiliki oleh suatu perusahaan di mana harga perolehannya atau nilai wajarnya harus diukur secara objektif (Munawir, 2007). Sehingga dapat disimpulkan apabila aset merupakan sesuatu yang bernilai bagi perusahaan.

2.4.3 Pengertian Aset Teknologi Informasi

Di dalam penelitiannya yang berjudul "*Develop Long-Term Competitiveness through IT Assets*", Jeanne Ross, Cynthia Mathis, dan Dale Goodhue mengemukakan bahwa terdapat tiga jenis aset utama yang harus diperhatikan oleh sebuah organisasi atau perusahaan apabila ingin tetap mempertahankan kehandalan sistem informasi yang dimiliki yang disebut dengan istilah "*The Three IT Assets*". Ketiga aset tersebut diantaranya sumber daya manusia, teknologi dan relasi.

a. Aset Sumber Daya Manusia
   Sumber daya manusia yang dimaksud adalah para staf penanggung jawab perencanaan dan pengembangan teknologi informasi yang ada pada sebuah organisasi maupun perusahaan, seperti seperti Divisi Teknologi Informasi, Departemen Sistem Informasi, atau bagian sejenis lainnya.
b. Aset Teknologi
   Aset teknologi ini meliputi seluruh infrastruktur teknologi informasi yang digunakan oleh organisasi maupun perusahaan termasuk perangkat keras (*hardware*) dan perangkat lunak (*sotfware*).
c. Aset Relasi
   Aset relasi yang dimaksud adalah hubungan antara teknologi informasi dengan orang-orang pada manajemen puncak yang memiliki wewenang untuk mengambil keputusan. Orang-orang tersebut biasanya terdiri dari para anggota direksi dan direktur yang bertanggung jawab terhadap terselenggaranya proyek-proyek teknologi informasi.

Berdasarkan tiga jenis aset utama teknologi informasi yang telah dijelaskan sebelumnya, seluruh infrastruktur teknologi informasi baik perangkat keras

(*hardware*) dan perangkat lunak (*sotfware*) merupakan aset organisasi maupun perusahaan yang digunakan secara bersama-sama. Infrastruktur teknologi informasi ini dianggap sangat penting karena merupakan tulang punggung (*backbone*) dalam menciptakan sebuah sistem yang terintegrasi, baik untuk keperluan operasional, pengembangan maupun pemeliharaan. Dengan demikian aset teknologi dapat didefinisikan sebagai keseluruhan infrastruktur teknologi informasi baik *hardware*, *software*, serta *database* yang tersimpan dan teratur di dalam sistem secara terpusat.

2.4.3.1 Jenis Aset Teknologi Informasi

Jika dilihat segi manfaat yang dirasakan, aset teknologi informasi terbagi menjadi dua jenis, yaitu aset *tangible* (berwujud) dan aset *intangible* (tidak berwujud).

a. Aset *Tangible*
   Aset *tangible* merupakan aset yang manfaatnya dapat diperoleh secara nyata oleh organisasi maupun perusahaan dan dapat langsung digunakan atau diaplikasikan untuk keuntungan bersama maupun pribadi. Contoh dari aset *tangible* adalah *hardware, database,* dan *server*.
b. Aset *Intangible*
   Aset *intangible* merupakan aset yang manfaatnya dapat diperoleh secara tidak nyata oleh organisasi maupun perusahaan. Contoh dari aset *intangible* adalah *software.*

2.4.3.2 Kategori Aset Teknologi Informasi

Menurut Albert, Dorofee, Steven dan Woody (2005) dalam bukunya OCTAVE-S telah membagi aset teknologi informasi menjadi empat kategori, yaitu:

a. Informasi
   Data yang didokumentasikan (kertas atau elektronik) atau kekayaan intelektual yang digunakan untuk memenuhi tujuan organisasi.
b. Sistem
   Kombinasi informasi, perangkat lunak, dan aset perangkat keras yang memproses dan menyimpan informasi. Setiap host, klien, atau server dapat dianggap sebagai sistem.
c. Layanan dan aplikasi
   Aplikasi dan layanan perangkat lunak (sistem operasi, aplikasi basis data, perangkat lunak jaringan, aplikasi kantor, aplikasi khusus, dll) yang digunakan untuk memproses, menyimpan, atau mengirim informasi.
d. Orang-orang
   Orang-orang dalam organisasi yang memiliki keterampilan, pengetahuan, dan pengalaman unik yang sulit diganti.

2.4.4 Pengertian Sistem

Menurut O'Brien (2002), sistem merupakan sekumpulan komponen-komponen yang saling berhubungan, dengan batasan yang jelas dan saling bekerja sama untuk mencapai tujuan bersama dengan menerima *input* serta menghasilkan *output* melalui proses transformasi yang terorganisir. Sedangkan menurut Gelinas dan Dull (2012), sistem merupakan seperangkat elemen independen yang bersama-sama mencapai tujuan tertentu atau spesifik. Sistem juga dikatakan sebagai kumpulan dari bagian-bagian yang saling terintegrasi satu dengan yang lainnya.

Dari pengertian-pengertian tersebut maka dapat disimpulkan bahwa sistem merupakan komponen-komponen atau bagian-bagian yang saling berkaitan, yang saling bekerja sama untuk mencapai suatu tujuan tertentu dengan cara menerima *input* dan menghasilkan *output* melalui suatu proses transformasi yang tersusun secara teratur atau terorganisir.

2.4.5 Pengertian Informasi

Menurut Jogiyanto (1999), informasi didefinisikan sebagai hasil dari pengolahan data menjadi suatu bentuk yang lebih berguna dan lebih berarti bagi penerimanya yang menggambarkan suatu kejadian- kejadian (*event*) yang nyata (*fact*) dan digunakan untuk proses pengambilan keputusan.

Selanjutnya McLeod (2001) menyatakan bahwa informasi merupakan data yang telah diolah atau diproses menjadi bentuk yang lebih memiliki arti bagi penerima serta bermanfaat bagi proses pengambilan keputusan yang dilakukan saat ini maupun masa yang akan datang. Sedangkan data terdiri dari fakta-fakta dan angka-angka yang secara relatif tidak berarti bagi pemakai.

Sehingga dapat disimpulkan bahwa informasi adalah sekumpulan data atau fakta yang telah diolah sehingga menjadi sesuatu yang lebih berguna dan menjadi informasi bagi orang yang membutuhkan untuk membantu dalam proses pengambilan keputusan.

2.4.6 Pengertian Sistem Informasi

Menurut O'Brien (2007), sistem informasi merupakan gabungan antara manusia, perangkat lunak, perangkat keras, jaringan komunikasi, dan sumber daya data yang saling terorganisir dalam mengumpulkan, mengubah, dan menyebarkan informasi dalam organisasi. Menurut Gondodiyoto (2007), sistem informasi dapat didefinisikan sebagai kumpulan elemen atau sumber daya dan jaringan yang saling berkaitan secara terpadu, dan terintegrasi dalam suatu hubungan hierarki tertentu yang bertujuan untuk mengolah data menjadi informasi.

Jadi, dapat disimpulkan bahwa sistem informasi merupakan sekumpulan komponen yang saling terintegrasi untuk mengolah, menghasilkan dan menyebarkan informasi di dalam sebuah organisasi.

2.4.6.1 Komponen Sistem Informasi

Menurut Jogiyanto (2007), komponen sistem informasi terbagi menjadi beberapa bagian antara lain:

a. Komponen Masukan (*Input*)
   Masukan (*input*) merupakan data yang masuk ke dalam sistem informasi. Komponen ini merupakan bahan dasar yang digunakan dalam proses pengolahan informasi.
b. Komponen Model
   Komponen model digunakan untuk memproses dan mengolah data. Informasi yang dihasilkan oleh sistem informasi berasal dari data yang diambil dari basis data yang kemudian diolah dengan menggunakan model-model tertentu. Model yang digunakan dalam sistem informasi ini dapat berupa model logika dan model matematika.
c. Komponen Keluaran (*Output*)
   Keluaran (*output*) merupakan produk yang dihasilkan dari sistem informasi yang berguna bagi penggunanya. *Output* tersebut dihasilkan dengan menggunakan data yang diperoleh dari basis data dan diproses dengan menggunakan model tertentu.
d. Komponen Teknologi
   Komponen teknologi merupakan komponen yang penting pada sistem informasi. Keberadaan teknologi mendukung sistem informasi untuk dapat menghasilkan informasi yang tepat waktu. Teknologi berfungsi untuk mempercepat sistem informasi dalam melakukan pemrosesan dan pengolahan data. Komponen teknologi dapat dikelompokkan menjadi 2 kategori, yaitu teknologi sistem komputer (*hardware* dan *software*) dan teknologi sistem telekomunikasi.
e. Komponen Basis Data
   Basis data (*database*) merupakan sekumpulan data yang saling berhubungan satu dengan yang lainnya, yang tersimpan pada perangkat keras komputer dan selanjutnya diolah atau diproses dengan menggunakan perangkat lunak.
f. Komponen Pengendalian (*Control*)
   Komponen pengendalin (*control*) digunakan untuk menjamin bahwa informasi yang dihasilkan oleh sistem informasi merupakan informasi yang tepat dan akurat. Dalam sistem informasi, sistem kontrol dapat diklasifikasikan sebagai sistem pengendalian umum (*general control system*) dan sistem pengendalian aplikasi (*application control system*).

2.4.7 Infrastruktur Teknologi Informasi

Menurut Turban, Rainer & Potter (2007), infrastruktur teknologi informasi merupakan fasilitas fisik yang terdiri dari komponen (*IT components*), layanan (*IT services*), dan personil teknologi informasi (*IT personnel*) yang mendukung keseluruhan organisasi. Komponen teknologi informasi terdiri dari perangkat keras (*hardware*), perangkat lunak (*software*) dan teknologi komunikasi yang

digunakan oleh personil teknologi informasi untuk dapat menghasilkan layanan teknologi informasi. Layanan teknologi informasi meliputi manajemen data.

2.4.7.1 Perangkat Keras (*hardware*)

Menurut O'Brien (2007), perangkat keras (*hardware*) mencakup seluruh peralatan fisik yang digunakan dalam memproses informasi. *Hardware* berkaitan dengan peralatan fisik dan media komunikasi untuk menghubungkan beberapa jaringan dan memproses paket data sehingga transmisi data lebih efektif. Sehingga dapat disimpulkan bahwa *hardware* merupakan seluruh perangkat fisik yang membentuk suatu sistem komputer dan segala perlengkapan yang saling berhubungan.

2.4.7.2 Perangkat Lunak (*software*)

Menurut Rainer (2013), perangkat lunak (*software*) merupakan sekumpulan program yang memungkinkan perangkat keras (*hardware*) untuk memproses data. Sedangkan menurut penjelasan Turban & Volonino (2012), perangkat lunak adalah sekumpulan aplikasi atau program yang memberikan instruksi kepada perangkat keras untuk memproses data atau masukan lain seperti perintah suara. Sehingga dapat disimpulkan bahwa perangkat lunak (*software*) adalah sekumpulan program atau aplikasi yang memberikan perintah kepada perangkat keras (*hardware*) untuk memproses data dan informasi.

2.4.7.3 Jaringan Komputer

Menurut Dede Sopandi (2008), jaringan komputer merupakan gabungan antara teknologi komputer dengan teknologi komunikasi. Sedangkan menurut Turban, Rainer dan Potter (2003), jaringan komputer merupakan suatu himpunan interkoneksi antara dua atau lebih dari komputer *autonomous* yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). Secara umum dapat dijelaskan bahwa jaringan komputer adalah sekumpulan komputer dan perangkat lain yang saling terhubung satu sama lainnya melalui media perantara seperti kabel maupun tanpa kabel (*wireless*). Dengan menggunakan jaringan komputer tersebut maka semua komputer yang terhubung akan dapat saling berbagi maupun bertukar data dan informasi.

2.5 Risiko Teknologi Informasi

2.5.1 Manajemen Keamanan

Keamanan merupakan hal penting yang perlu diperhatikan dalam mengoperasikan sistem informasi dan teknologi informasi. Manajemen keamanan dilakukan untuk melakukan pencegahan terhadap ancaman dan gangguan baik dari dalam maupun dari luar serta untuk mendeteksi dan memperbaiki dampak yang ditimbulkan akibat risiko yang terjadi.

Menurut O'Brien (2006), manajemen keamanan merupakan salah satu tanggung jawab yang paling penting dari manajemen organisasi untuk

memastikan keamanan aktivitas atau proses bisnis yang dijalankan dengan menggunakan teknologi informasi sebagai fasilitas. Manajemen keamanan bertujuan untuk memastikan akurasi, integrasi dan keamanan baik proses maupun sumber daya dari seluruh sistem informasi. Sehingga aktivitas manajemen keamanan yang baik dan efektif akan dapat meminimalkan kemungkinan kesalahan, penipuan dan kerugian pada sistem informasi yang menghubungkan organisasi dengan pelanggan, *supplier,* dan *stakeholder* mereka.

2.5.2 Manajemen Keamanan Informasi

Menurut Alberts, C dan Dorofee.A (2002) di dalam bukunya menjelaskan bahwa terdapat empat pendekatan yang biasa digunakan terkait dengan keamanan informasi, diantara lain:

1. Penilaian kerentanan (*Vulnerability Assessment*)
   Pada pendekatan ini dilakukan pemeriksaan terhadap teknologi dasar yang digunakan, serta kebijakan dan prosedur yang dimiliki oleh organisasi maupun perusahaan. Hal ini termasuk dalam menganalisis keamanan lingkungan komputer internal dari serangan-serangan yang dapat berasal baik dari sisi internal maupun eksternal. Penilaian berbasis teknologi ini secara umun dilakukan dengan:
   a. Menggunakan suatu standar atau kerangka kerja tertentu
   b. Menilai seluruh infrastruktur komputasi
   c. Menggunakan software untuk menganalisis infrastruktur beserta dengan komponennya
   d. Analisis risiko atau kerentanan yang terdeteksi serta mencari cara untuk mengatasinya
2. Audit Sistem Informasi
   Pada dasarnya pendekatan audit sistem informasi merupakan suatu penilaian independen yang dilakukan dari kontrol internal organisasi maupun perusahaan untuk menyatakan bahwa informasi yang dimiliki akurat dan valid.
3. Evaluasi Risiko Keamanan Informasi
   Seperti halnya manajemen risiko, evaluasi risiko keamanan informasi dilakukan dengan melaksanakan aktivitas identifikasi risiko keamanan informasi, analisis risiko untuk menentukan prioritas hingga melakukan kontrol terhadap variasi rencana yang digunakan untuk memilih *corrective actions* yang tepat. Evaluasi risiko merupakan langkah pertama yang dilakukan dalam aktivitas manajemen risiko. Evaluasi risiko keamanan informasi harus mampu mengidentifikasi baik masalah organisasional maupun teknologikal secara efektif. Hal tersebut dilakukan dengan mengidentifikasi infrastruktur komputer serta bagaimana orang-orang di dalam organisasi maupun perusahaan menggunakannya untuk menunjang pekerjaan mereka.
   Pendekatan dengan cara evaluasi ini dilakukan dengan menilai kerentanan internal organisasi maupun perusahaan termasuk menilai sumber risiko baik yang berasal dari sisi internal maupun eksternal serta

berbasis elektronik atau masyarakat. Evaluasi yang dilakukan ini berfokus pada aspek:

a. Memeriksa praktik yang dilakukan oleh organisasi maupun perusahaan terkait dengan keamanan untuk mengidentifikasi kekuatan dan kelemahan yang dapat menciptakan atau mengurangi risiko.
b. Memeriksa teknologi sistem, kebijakan, dan keamanan fisik
c. Memeriksa infrastruktur teknologi informasi untuk menentukan kemampuan kerentanan teknologi

4. Pengelolaan Penyedia Layanan
   Pengelolaan penyedia layanan bergantung kepada keahlian manusia dalam mengelola sistem dan jaringan yang dimiliki oleh organisasi maupun perusahaan. Biasanya pengelolaan pada layanan keamanan yang dilakukan secara proaktif akan melakukan pemantauan dan perlindungan terhadap infrastruktur. Pengelolaan jenis ini akan secara aktif menanggapi gangguan setelah gangguan tersebut terjadi.

2.5.3 Aspek Keamanan Informasi

Dalam mengembangkan sebuah sistem informasi, keamanan informasi merupakan aspek penting yang harus diperhatikan untuk memastikan bahwa sistem informasi tersebut tidak menimbulkan kerugian bagi kepentingan para pengguna seperti kebocoran data rahasia dan sebagainya. Terdapat beberapa kriteria aspek keamanan yang sering disebut sebagai C.I.A *triangle model,* yaitu:

1. *Confidentiality* (Kerahasiaan)
   Aspek ini berhubungan kerahasiaan data dan informasi penting yang tersimpan pada sistem. Data dan informasi tersebut hanya boleh diakses oleh orang-orang tertentu yang memiliki hak akses. Aspek ini menjamin bahwa hanya orang-orang yang memiliki hak akses yang dapat mengakses siste.
2. *Integrity* (Integritas)
   Aspek ini berhubungan dengan integritas, kelengkapan dan konsistensi data yang tersimpan di dalam sistem. Aspek ini memastikan bahwa data dan informasi yang tersimpan tidak boleh dirubah oleh orang yang tidak memiliki hak akses. Hal ini bertujuan untuk menjaga data dan informasi dari kerusakan dan ancaman-ancaman lain yang dapat menyebabkan perubahan yang tidak sesuai.
3. *Availability* (Ketersediaan)
   Aspek ini berhubungan dengan ketersediaan data dan informasi yang tersimpan pada sistem ketika dibutuhkan. Aspek ini juga menjamin bahwa pengguna akan dapat mengakses data dan informasi yang dibutuhkan tanpa adanya gangguan serta tidak dalam format yang tidak dapat digunakan.

2.5.4 Kategori Risiko Teknologi Informasi

Dalam penerapannya, 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. Contoh dari ancaman terhadap keamanan adalah sabotase, kejahatan komputer, terorisme cyber dan kebocoran internal.
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 sistem, kegagalan terhadap perangkat lunak maupun keras, ancaman eksternal atau bencana alam.
d. Performa
   Risiko terhadap informasi dimana informasi tidak tersedia saat diperlukan. Hal tersebut diakibatkan oleh permintaan terhadap informasi yang tinggi, arsitektur terdistribusi serta topografi teknologi informasi yang beragam.
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. Risiko jenis ini berkaitan dengan aturan pemerintah, panduan aturan pemerintah serta kebijakan internal yang berlaku.

2.5.5 Manajemen Risiko Teknologi Informasi

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, di mana elemen penting yang harus dipertimbangkan adalah:

a. Strategi dan Kebijakan
   Strategi dan kebijakan manajemen risiko teknologi informasi diperlukan untuk menentukan tujuan dari manajemen risiko teknologi informasi secara keseluruhan. Strategi juga digunakan untuk membangun prioritas serta menyadari pentingnya penerapan manajemen risiko teknologi

informasi. Selain itu kebijakan juga digunakan untuk memastikan cakupan area potensial terhadap risiko teknologi informasi serta menyediakan landasan pembuatan peraturan dan prinsip untuk mengelola risiko.

b. Peran dan Tanggung Jawab
   Menentukan peran dan tanggung jawab yang harus dikerjakan untuk masing-masing orang yang ada di dalam organisasi terlebih dahulu, kemudian memilih orang yang tepat untuk ditempatkan pada posisi tersebut.

c. Proses dan Pendekatan
   Manajemen risiko memiliki *lifecycle* yang terdiri dari beberapa tahapan. Tahapan-tahapan siklus hidup tersebut kemudian dikembangkan dengan beberapa langkah yang berbeda untuk berbagai jenis risiko:
   1. Identifikasi atau Penemuan
      Mengidentifikasi risiko teknologi informasi berdasarkan penjelasan dan petunjuk yang diberikan oleh bagian manajerial.
   2. Penilaian atau Analisis
      Memahami risiko berdasarkan portfolio risiko teknologi informasi secara keseluruhan. Kemudian melakukan penilaian atau analisis terhadap kemungkinan terjadinya risiko serta dampak potensial yang dihasilkan terhadap keberlangsungan proses bisnis.
   3. Perawatan
      Menentukan langkah yang tepat dan sesuai untuk melakukan perencanaan penanganan risiko dan menyelesaikan tindakan-tindakan yang diperlukan dalam pelaksanaannya.
   4. Pemantauan dan Tinjauan
      Melakukan proses tindak lanjut berupa pemantauan dan peninjauan terhadap rencana yang dilakukan. Hal ini bertujuan untuk memastikan bahwa rencana yang dilakukan berjalan sesuai dengan yang diharapkan. Selain itu, proses ini dilakukan untuk memahami perubahan-perubahan yang mungkin terjadi lebih lanjut terhadap portfolio risiko.

d. Orang dan Peforma
   Dalam melakukan manajemen risiko, kemampuan dan pengetahuan orang-orang di dalam manajemen harus dikembangkan dan dipelihara karena hal tersebut akan berpengaruh dan menentukan performa mereka. Proses pengembangan dan pemeliharaan ini memerlukan kombinasi antara pendidikan dan pelatihan dalam menanggulangi risiko teknologi informasi yang disesuaikan dengan peran dan tanggung jawab mereka.

e. Implementasi dan Pengembangan
   Dalam menerapkan dan mengembangkan menajemen risiko teknologi informasi dalam suatu organisasi, perlu adanya pemberian informasi terhadap orang-orang yang ada di dalamnya. Hal ini akan membantu untuk meyakinkan mereka tentang pentingnya pengelolaan risiko untuk organisasi.

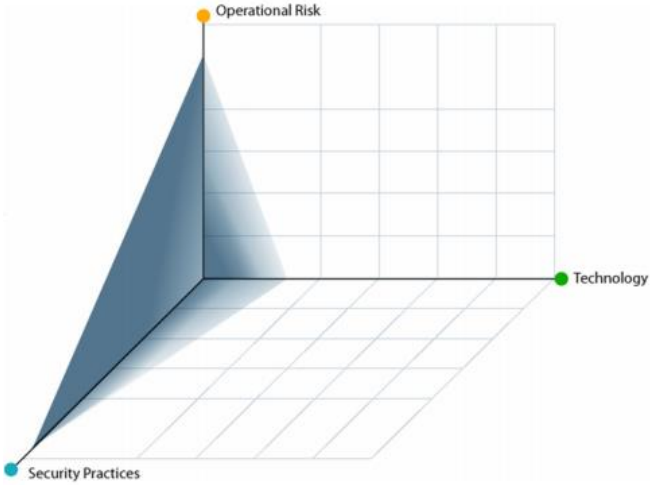
2.6 OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*)-S

Terdapat beberapa kerangka kerja yang dapat digunakan untuk menerapkan manajemen risiko pada sebuah organisasi atau perusahaan. Salah satu kerangka kerja yang dapat membantu penerapan manajemen risiko adalah OCTAVE.

Menurut Albert, Dorofee, Steven dan Woody (2005), OCTAVE (*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.

Pendekatan OCTAVE didorong oleh dua aspek diantaranya risiko operasional dan praktik keamanan. Aspek teknologi hanya diperiksa berdasarkan keterkaitannya dengan praktik keamanan. OCTAVE difokuskan pada risiko organisasi, hasil praktik dan strategi keamanan yang saling berkaitan. Teknik ini memanfaatkan pengetahuan beberapa pihak tentang praktik dan proses keamanan terkait organisasi untuk melihat dan memahami keadaan praktik keamanan yang telah dijalankan saat ini. Hal ini juga bertujuan untuk memahami, menilai dan menangani risiko keamanan informasi dari sudut pandang organisasi. Dengan menggunakan OCTAVE, organisasi maupun perusahaan akan dapat membuat keputusan untuk perlindungan informasi berdasarkan risiko terhadap kerahasiaan, integritas dan ketersediaan aset-aset yang berkaitan dengan informasi penting (*critical information*). Semua aspek risiko yang diperhitungkan dalam pengambilan keputusan akan memungkinkan organisasi ataupun perusahaan untuk mencocokkan strategi perlindungan dengan risiko keamanannya. (Albert, 2003).

OCTAVE merupakan sebuah pendekatan terhadap evaluasi risiko keamanan informasi yang terarah, sistematik, komprehensif, serta bersifat *self-directed*. Hal tersebut berarti bahwa orang-orang dari sebuah organisasi memiliki tanggung jawab untuk menetapkan strategi keamanan untuk organisasi tersebut. Aktivitas pendekatan OCTAVE dipimpin oleh tim analisis interdisipliner yang anggotanya terdiri dari personil teknologi informasi dan bisnis organisasi yang dinilai. Dimana kedua bagian tersebut akan bekerja sama untuk menangani kebutuhan keamanan organisasi dengan menyeimbangkan tiga aspek utama yaitu, risiko operasional, praktik keamanan, dan teknologi. (Albert, 2003).



Gambar 2.2 Hubungan Antara Tiga Aspek OCTAVE

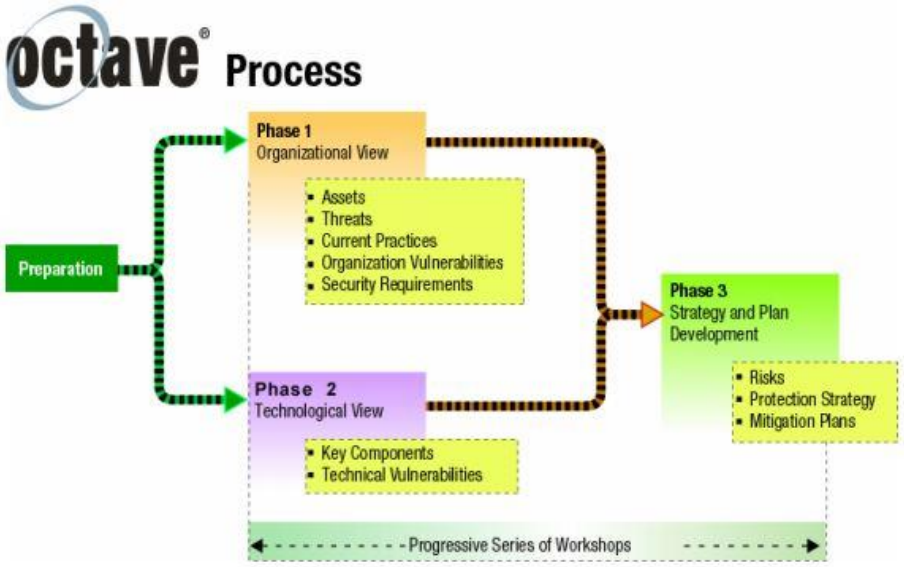
(Sumber: OCTAVE)

Terdapat beberapa perbedaan yang membedakan OCTAVE dengan pendekatan lainnya seperti yang tertera pada tabel di bawah ini:

Tabel 2.2 Perbedaan OCTAVE dengan Pendekatan lainnya

OCTAVE	Metode Lain
Terdapat tahapan peningkatan sistem informasi manajemen risiko.	Tidak memiliki fase peningkatan risiko sistem informasi (CRAMM, CORAS) (Bornman & Labuschagne, 2006)
Terdapat prosedur formal untuk proses menerima risiko.	Tidak terdapat prosedur formal untuk proses "menerima risiko" (CRAMM, CORAS, COBIT) (Bornman & Labuschagne, 2006)
Berfokus pada evaluasi risiko sistem informasi.	Fokus pada proses membangun Tata Kelola TI (COBIT) (Bornman & Labuschagne, 2006)
Mempertimbangkan "Orang" sebagai salah satu aset dalam proses evaluasi risiko sistem informasi.	"Orang" tidak termasuk sebagai aset dalam proses evaluasi risiko sistem informasi. (Alberts, Dorofee, Stevens, & Woody, 2005)

Menurut Panduan Penerapan Metode OCTAVE v2.0, OCTAVE dibagi menjadi tiga kriteria yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro. Pembagian tersebut didasarkan pada skala organisasi. OCTAVE dirancang dan dikembangkan untuk organisasi atau perusahaan besar yang memiliki lebih dari 300 karyawan, OCTAVE-S dirancang dan dikembangkan untuk organisasi kecil yang memiliki 20 hingga 80 orang karyawan, sedangkan OCTAVE Allegro dirancang dan dikembangkan untuk organisasi yang memiliki kurang dari 10 orang karyawan teknologi informasi atau bahkan tidak ada sama sekali.



Gambar 2.3 Proses OCTAVE

(Sumber: OCTAVE)

Kerangka kerja OCTAVE-S memiliki tiga tahapan yang sama dengan OCTAVE, yaitu membangun proses profil ancaman berdasarkan aset yang ada (*Build Asset-Based Threat Profiles*), melakukan identifikasi kerentanan dari infrasruktur (*Identify Infrastructure Vulnerabilities*), dan mengembangkan rencana dan strategi keamanan (*Develop Security Strategy and Plans*). Perbedaan antara OCTAVE dan OCTAVE-S terletak pada proses yang ada di dalamnya.

Dibawah ini merupakan penjelasan dari tahapan-tahapan tersebut:

2.6.1 Fase 1 : Membangun Profil Ancaman Berbasis Aset

Tabel 2.3 Fase Membangun Profil Ancaman Berbasis Aset

Fase	Proses	Aktivitas
Fase 1 : Membangun Profil Ancaman Berbasis Aset	Proses 1: Identifikasi Informasi Organisasi	S1.1 Menetapkan Kriteria Evaluasi Dampak
		S1.2 Mengidentifikasi Aset Organisasi
		S1.3 Mengevaluasi Praktik Keamanan Organisasi
	Proses 2: Membuat Profil Ancaman	S2.1 Memilih Aset Kritis
		S2.2 Mengidentifikasi Kebutuhan Keamanan untuk Aset Kritis
		S2.3 Mengidentifikasi Ancaman terhadap Aset Kritis

Pada tahapan ini dilakukan evaluasi terhadap aspek organisasi. Evaluasi tersebut dimulai dengan melakukan identifikasi terhadap informasi organisasi yang akan digunakan untuk mendefinisikan profil ancaman. Kemudian mendefinisikan kriteria evaluasi dampak yang akan digunakan untuk mengevaluasi risiko. Selanjutnya mengidentifikasi aset organisasi yang penting dan melakukan evaluasi praktik keamanan organisasi yang ada saat ini. Setelah dilakukan pengumpulan informasi maka kemudian akan dipilih beberapa (tiga sampai lima) aset penting untuk dianalisis secara mendalam berdasarkan kepentingan relatif organisasi terhadap masing-masing aset tersebut.

2.6.1.1 Proses 1: Identifikasi Informasi Organisasi

Proses ini berfokus pada pengembangan kriteria evaluasi dampak, identifikasi aset-aset organisasi, dan evaluasi praktik keamanan organisasi. Di dalam proses ini terdapat beberapa aktivitas yang akan dilaksanakan, yaitu:

a. S1.1 Menetapkan Kriteria Evaluasi Dampak

Membuat beberapa kriteria pengukuran dampak yang digunakan untuk mengevaluasi pengaruh risiko pada organisasi. Kriteria evaluasi dampak merupakan serangkaian ukuran kualitatif yang digunakan untuk menilai dampak setiap risiko pada misi organisasi dan tujuan bisnis. Kriteria evaluasi dampak menentukan rentang dampak tinggi, sedang, dan rendah untuk suatu organisasi. Terdapat beberapa kriteria dampak yang dapat dijadikan acuan diantaranya reputasi atau kepercayaan pelanggan terhadap organisasi atau perusahaan; kehidupan atau kesehatan pelanggan; keuangan; denda atau aturan hukum yang berlaku; produktifitas karyawan; dan lain sebagainya.

b. S1.2 Mengidentifikasi Aset Organisasi

Mengidentifikasi aset-aset organisasi atau perusahaan yang dapat berupa sistem, informasi, layanan dan aplikasi yang dibutuhkan oleh organisasi tersebut untuk menunjang tugas dan fungsinya. Kemudian mengidentifikasi aset manusia atau orang-orang yang ada di dalam organisasi.

c. S1.3 Mengevaluasi Praktik Keamanan Organisasi

Albert, dkk (2005) menjelaskan dalam bukunya OCTAVE-S bahwa praktik kemanan merupakan tindakan yang digunakan untuk membantu memulai, menerapkan dan menjaga keamanan dalam suatu organisasi atau perusahaan. Terdapat dua jenis area praktik keamanan yang disebutkan oleh OCTAVE, diantaranya praktik strategis (*strategic practices*) dan praktik operasional (*operational practices*). Praktik strategis (*strategic practices*) merupakan praktik keamanan yang berfokus pada masalah organisasi di tingkat kebijakan (*policy level*). Sedangkan praktik operasional (*operational practices*) merupakan praktik keamanan yang berfokus pada masalah-masalah yang berkaitan dengan teknologi.

Pada aktivitas ini dilakukan peninjauan pernyataan di setiap area praktik keamanan pada *Security Practices Worksheet*, kemudian memberikan penilaian dengan kriteria:

- *Very Much* - pernyataan ini mewakili praktik saat ini di organisasi.
- *Somewhat* - pernyataan secara sebagian menggambarkan praktik saat ini di organisasi, namun beberapa aspek pernyataan tidak mewakili praktik saat ini di organisasi.
- *Not At All* - Pernyataan itu tidak mewakili praktik saat ini di organisasi sama sekali.

Selanjutnya menetapkan status *stoplight* pada setiap area praktik keamanan. Status *stoplight* tersebut akan mencerminkan seberapa baik praktik keamanan yang telah diterapkan oleh organisasi pada setiap area.

- *Green* - organisasi telah melaksanakan praktik keamanan pada area tersebut dengan sangat baik sehingga tidak membutuhkan perbaikan.
- *Yellow* - organisasi hanya melaksanakan sebagian praktik keamanan pada area tersebut atau hanya mencapai batas tertentu sehingga membutuhkan sedikit perbaikan.
- *Red* - organisasi tidak melaksanakan praktik keamanan pada area tersebut sehingga membutuhkan perbaikan yang signifikan.

2.6.1.2 Proses 2: Membuat Profil Ancaman

Proses ini berfokus untuk memilih tiga sampai lima aset penting yang berkaitan dengan informasi serta menentukan kebutuhan keamanan dan profil ancaman untuk aset tersebut. Di dalam proses ini terdapat beberapa aktivitas yang akan dilaksanakan, yaitu:

a. S2.1 Memilih Aset Kritis

Pada aktivitas ini akan dilakukan analisis terhadap aset-aset yang telah diidentifikasi dalam *Asset Identification Worksheet.* Kemudian memilih aset-aset yang penting bagi organisasi atau perusahaan. Aset mana yang berisiko menimbulkan dampak kerugian yang besar pada organisasi atau perusahaan apabila aset tersebut terancam. Selain itu mengidentifikasi siapa yang menggunakan dan bertanggung jawab terhadap aset tersebut, serta apakah ada aset lain yang memiliki keterkaitan dengan aset penting yang dipilih.

b. S2.2 Mengidentifikasi Kebutuhan Keamanan untuk Aset Kritis

Pada aktivitas ini dilakukan pencatatan kebutuhan keamanan untuk setiap aset kritis. Kebutuhan keamanan adalah pernyataan yang menggambarkan kualitas aset yang berkaitan dengan informasi yang penting bagi suatu organisasi. Kebutuhan keamanan yang umum dibutuhkan oleh masing-masing aset kritis adalah kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*).

Kebutuhan keamanan tersebut berfokus pada kebutuhan apa yang seharusnya ada untuk suatu aset, bukan apa yang sedang diterapkan saat ini. Selain itu hal yang harus dipertimbangkan saat menyusun pernyataan untuk masing-masing aset kritis adalah kebutuhan keamanan mana yang paling penting untuk aset yang teridentifikasi.

c. S2.3 Mengidentifikasi Ancaman terhadap Aset Kritis

Ancaman merupakan indikasi adanya peristiwa potensial yang tidak diinginkan. Ancaman mengacu pada situasi di mana seseorang dapat melakukan sesuatu yang tidak diinginkan (peretas yang menyerang *server e-mail* organisasi) atau kejadian alami dapat menyebabkan hasil yang tidak diinginkan (bencana alam). Ancaman direpresentasikan dengan menggunakan beberapa properti, seperti aset yang teridentifikasi, jalur akses, aktor yang melakukan, motif yang dimiliki serta dampak yang dihasilkan dari ancaman tersebut.

Masing-masing kategori aset kritis baik sistem, informasi, layanan, aplikasi dan manusia memiliki *Risk Profile Worksheet* yang unik dan berbeda antara satu sama lain. Langkah pertama yang harus dilakukan ketika melaksanakan aktivitas ini adalah memilih *worksheet* yang tepat untuk masing-masing aset kritis. Kemudian melengkapi semua skema ancaman atau *threat tree* yang sesuai untuk setiap aset penting dengan mempertimbangkan cabang mana yang memiliki kemungkinan ancaman terhadap aset yang tidak dapat diabaikan dan cabang mana terdapat kemungkinan ancaman yang dapat diabaikan atau tidak ada kemungkinan ancaman terhadap aset.

Selanjutnya adalah melengkapi kategori *Human Actors Using Network Access* dan *Human Actors Using Physical Access.* Pada tahapan ini dilakukan identifikasi terhadap motif masing-masing aktor pada masing-masing kategori, baik aktor yang berasal dari dalam organisasi maupun yang berasal dari luar organisasi, dengan motif yang baik disengaja maupun tidak. Kemudian menganalisis aktor manakah yang paling berpotensi menimbulkan ancaman bagi organisasi pada masing-masing kategori.

Terdapat beberapa kriteria yang diberikan dalam menilai seberapa besar motif orang tersebut dalam bertindak, diantaranya:

- *High* - Aktor memiliki tujuan yang jelas untuk menyerang organisasi dengan menetapkan aset kritis sebagai target serangan. Selain itu mereka akan melakukan berbagai cara untuk memastikan tujuan mereka berhasil.
- *Medium* - Aktor memiliki tujuan yang jelas untuk menyerang organisasi namun menetapkan target serangan secara umum. Selain itu mereka juga memiliki *exit startegy* secara eksplisit maupun implisit untuk menentukan kapan mereka akan menghentikan serangan.
- *Low* - Aktor memiliki tujuan yang jelas untuk menyerang organisasi namun tidak menetapkan target serangan secara spesifik, menargetkan aset apa pun yang dapat diserang dengan mudah. Selain itu mereka akan melakukan berbagai cara untuk memastikan tujuan mereka berhasil.

Berikutnya adalah memastikan seberapa yakin pernyataan motif dibuat dengan memberikan penilaian dengan kriteria berikut ini:

- *Very* - Terdapat data obyektif dalam jumlah besar yang dapat digunakan sebagai pendukung.
- *Somewhat* - Terdapat data obyektif dalam jumlah terbatas yang dapat digunakan sebagai pendukung.
- *Not At All* - Terdapat sedikit atau bahkan tidak ada data obyektif yang dapat digunakan sebagai pendukung.

Langkah selanjutnya adalah menentukan seberapa sering ancaman tersebut terjadi di masa lalu, sebagai contoh berapa kali terjadi dalam jangka waktu satu tahun. Langkah tersebut dilakukan dengan meninjau data obyektif serta data subjektif yang dimiliki. Data objektif dapat berupa catatan insiden, sedangkan data subjektif dapat berupa pernyataan yang dibuat berdasarkan pendapat para karyawan yang mengingat kapan insiden terjadi. Kemudian menilai seberapa akurat data tersebut untuk mendukung pembuatan pernyataan motif dengan tiga kriteria yang sama dengan kriteria yang digunakan untuk menilai tingkat keyakinan, yaitu *very, somewhat* dan n*ot at all*.

2.6.2 Fase 2 : Mengidentifikasi Kerentanan Infrastruktur

Tabel 2.4 Fase Mengidentifikasi Kerentanan Infrastruktur

Fase	Proses	Aktivitas
Fase 2: Mengidentifikasi Kerentanan Infrastruktur	Proses 3: Memeriksa Infrastruktur Komputasi yang Berhubungan dengan Aset Kritis	S3.1 Memeriksa Jalur Akses
		S3.2 Menganalisis Proses Terkait dengan Teknologi

Pada tahapan ini, akan dilakukan peninjauan *high-level* terhadap infrastruktur komputasi organisasi yang berfokus pada sejauh mana keamanan dipertimbangkan oleh pengelola infrastruktur. Pertama-tama, melakukan analisis tentang bagaimana orang-orang menggunakan infrastruktur komputasi yang ada untuk mengakses aset kritis hingga siapa yang bertanggung jawab untuk mengkonfigurasi dan merawat komponen-komponen tersebut.

2.6.2.1 Proses 3: Memeriksa Infrastruktur Komputasi yang Berhubungan dengan Aset Kritis

Proses ini berfokus untuk menganalisis jalur akses dalam sistem yang mendukung aset kritis dan menentukan seberapa baik proses terkait teknologi mereka dalam melindungi aset tersebut. Di dalam proses ini terdapat dua aktivitas yang akan dilaksanakan, yaitu:

a. S3.1 Memeriksa Jalur Akses

Langkah pertama yang harus dilakukan pada aktivitas ini adalah menentukan dan menetapkan sistem yang memiliki keterkaitan paling erat dengan aset kritis, kemudian mencari tahu di mana sistem tersebut disimpan dan diproses. Selain itu juga melakukan identifikasi terhadap beberapa sistem lain yang berkaitan dengan aset kritis.

Selanjutnya adalah melakukan identifikasi terhadap komponen-komponen apa saja yang menjadi bagian dari sistem diatas seperti *server, internal network, on-site workstation*, laptop, dan lain-lain. Langkah berikutnya adalah mengidentifikasi bagaimana informasi dan aplikasi dari sistem ditransmisikan kepada orang-orang yang mengakses sistem tersebut. Jenis komponen apa saja yang digunakan untuk mengirimkan informasi dan aplikasi dari sistem tersebut, seperti jaringan internal, jaringan eksternal atau melalui media yang lain.

Kemudian mengidentifikasi komponen apa saja yang digunakan oleh orang-orang untuk dapat mengakses sistem tersebut, seperti *on-site workstation*, laptop, komponen *wireless*, dan lain-lain. Dalam menentukan perangkat-perangkat tersebut, hal yang perlu diperhatikan adalah lokasi *access point* dari jaringan yang digunakan oleh organisasi atau perusahaan, seperti jaringan internal maupun eksternal.

Langkah berikutnya adalah menentukan lokasi penyimpanan data atau informasi yang dimiliki oleh sistem yang dipilih. Penyimpanan tersebut bertujuan sebagai cadangan apabila diperlukan, seperti menggunakan media penyimpanan internal, eksternal atau yang lainnya. Terakhir adalah mengidentifikasi sistem apa saja yang juga ikut mengakses informasi, layanan, atau aplikasi dari sistem tersebut, serta komponen apa saja yang dapat digunakan untuk melakukan akses tersebut.

b. S3.2 Menganalisis Proses Terkait dengan Teknologi

Langkah pertama yang dilakukan dalam aktivitas ini adalah mengidentifikasi kembali komponen apa saja yang memiliki keterkaitan dengan aset kritis. Kemudian mengidentifikasi kembali aset-aset kritis apa saja yang memiliki keterkaitan dengan komponen-komponen tersebut. Selanjutnya melakukan identifikasi terhadap siapa saja yang bertanggung jawab dalam memelihara atau *maintenance* serta bertanggung jawab terhadap keamanan untuk masing-masing komponen tersebut.

Kemudian mengidentifikasi dan menganalisis tentang sejauh mana organisasi mempertimbangkan keamanan ketika melakukan konfigurasi dan memelihara masing-masing komponen. Setelah itu memberikan penilaian terhadap pernyataan yang telah dibuat tersebut berdasarkan kriteria yang telah ditentukan, yaitu:

- *Very Much* - Terdapat data obyektif dalam jumlah besar yang dapat digunakan sebagai pendukung.

- *Somewhat* - Terdapat data obyektif dalam jumlah terbatas yang dapat digunakan sebagai pendukung.
- *Not At All* - Terdapat sedikit atau bahkan tidak ada data obyektif yang dapat digunakan sebagai pendukung.
- *Don't know* - Tidak memiliki pengalaman dan keahlian yang cukup untuk membuat perkiraan yang sesuai.

Selanjutnya mencatat sumber data serta cara yang digunakan untuk mendapatkan data tersebut. Terdapat beberapa cara yang dapat digunakan untuk mencari sumber data yang dibutuhkan, diantaranya:

- *Formal Techniques* - menggunakan teknik pengumpulan data dan analisis yang ketat untuk mencapai kesimpulan. Seperti menggunakan teknik evaluasi atau analisis formal lainnya.
- *Informal Means* - melakukan evaluasi singkat untuk mencapai kesimpulan. Teknik ini dapat dijalankan dengan melakukan evaluasi kerentanan yang sangat terbatas pada infrastruktur komputasi, melakukan tinjauan terbatas atau audit pada komponen-komponen.
- *Other* - melakukan pengumpulan data dengan cara yang lainnya.

2.6.3 Fase 3 : Mengembangkan Strategi Perlindungan dan Rencana Keamanan

Tabel 2.5 Fase Mengembangkan Strategi dan Rencana Keamanan

Fase	Proses	Aktivitas
Fase 3 : Mengembangkan Strategi dan Rencana Keamanan	Proses 4: Identifikasi dan Analisis Risiko	S4.1 Mengevaluasi Dampak Ancaman
		S4.2 Menetapkan Kriteria Evaluasi Kemungkinan
		S4.3 Mengevaluasi Kemungkinan Ancaman
	Proses 5: Mengembangkan Strategi Perlindungan dan Rencana Mitigasi	S5.1 Menjelaskan Strategi Perlindungan Terkini
		S5.2 Memilih Pendekatan Mitigasi
		S5.3 Mengembangkan Rencana Mitigasi Risiko
		S5.4 Mengidentifikasi Perubahan terhadap Strategi Perlindungan
		S5.5 Mengidentifikasi Langkah Selanjutnya

Pada tahapan ini, akan dilakukan identifikasi risiko terhadap aset kritis organisasi dan apa yang harus dilakukan terhadap risiko tersebut. Berdasarkan analisis informasi yang dikumpulkan, selanjutnya membuat strategi perlindungan untuk organisasi dan menentukan rencana mitigasi untuk mengatasi risiko terhadap aset kritis.

2.6.3.1 Proses 4: Identifikasi dan Analisis Risiko

Pada proses ini akan dilakukan evaluasi pada semua risiko untuk dampak yang ditimbulkan dan probabilitasnya. Di dalam proses ini terdapat tiga aktivitas yang akan dilaksanakan, yaitu:

a. S4.1 Mengevaluasi Dampak Ancaman

Sebelum mengevaluasi dampak potensial pada organisasi yang akan dihasilkan dari ancaman terhadap aset kritis, maka diperlukan peninjauan informasi tentang aset dan ancaman penting yang telah didokumentasikan sebelumnya. Informasi yang perlu ditinjau kembali diantaranya ancaman untuk masing-masing aset kritis; konteks ancaman seperti aktor yang berpotensi untuk menimbulkan ancaman, motif yang dimiliki, serta catatan risiko yang terjadi di masa lalu; serta catatan tambahan lainnya yang sekiranya diperlukan.

Selain itu peninjauan informasi juga dilakukan pada kebutuhan keamanan untuk masing-masing aset kritis, serta informasi mengenai setiap dampak ancaman yang akan diterima oleh organisasi dan tujuan bisnis organisasi. Seperti dampak terhadap reputasi organisasi dan kepercayaan pelanggan, regulasi atau hukum terkait hingga produktifitas yang dimiliki oleh setiap individu di dalam organisasi.

Kemudian melakukan penilaian terhadap dampak-dampak yang muncul dengan menggunakan kriteria yang telah disediakan, diantara lain:

- "H" untuk setiap dampak tinggi (*High*)
- "M" untuk setiap dampak sedang (*Medium*)
- "L" untuk setiap dampak rendah (*Low*)

b. S4.2 Menetapkan Kriteria Evaluasi Kemungkinan

Kriteria evaluasi probabilitas merupakan serangkaian ukuran kualitatif yang digunakan untuk memperkirakan kemungkinan terjadinya ancaman. Kriteria evaluasi kemungkinan menentukan rentang frekuensi untuk probabilitas tinggi, sedang, dan rendah. Ukuran tersebut menunjukkan seberapa sering ancaman terjadi selama jangka waktu yang sama.

Aktivitas ini bertujuan untuk menentukan ukuran probabilitas berdasarkan seberapa sering ancaman kemungkinan terjadi. Hal tersebut dapat diperoleh dengan melihat kembali informasi mengenai jenis ancaman terhadap aset kritis dan seberapa sering setiap ancaman tersebut telah terjadi di masa lalu. Kemudian memberikan penilaian terhadap probabilitas terjadinya masing-

masing ancaman risiko dengan menggunakan kriteria yang telah ditentukan seperti tinggi (*high*), sedang (*medium*), dan rendah (*low*).

c. S4.3 Mengevaluasi Kemungkinan Ancaman

Aktivitas berikutnya adalah menyesuaikan perkiraan probabilitas yang telah dibuat untuk masing-masing ancaman risiko dengan keakuratan data yang digunakan sebagai pendukung dengan memberikan penilaian dengan kriteria seperti berikut ini:

- *Very Much* - Terdapat data obyektif dalam jumlah besar yang dapat digunakan sebagai pendukung.
- *Somewhat* - Terdapat data obyektif dalam jumlah terbatas yang dapat digunakan sebagai pendukung.
- *Not At All* - Terdapat sedikit atau bahkan tidak ada data obyektif yang dapat digunakan sebagai pendukung.

2.6.3.2 Proses 5: Mengembangkan Strategi Perlindungan dan Rencana Mitigasi

Pada proses ini dilakukan pengembangan strategi perlindungan menyeluruh dan rencana mitigasi risiko berbasis pada praktik keamanan. Di dalam proses ini terdapat lima aktivitas yang akan dilaksanakan, yaitu:

a. S5.1 Menjelaskan Strategi Perlindungan Terkini

Strategi perlindungan mendefinisikan strategi keseluruhan yang digunakan oleh organisasi untuk mengaktifkan, memulai, menerapkan, dan menjaga keamanan internal mereka. Strategi perlindungan menentukan bagaimana suatu organisasi bermaksud untuk meningkatkan atau mempertahankan tingkat keamanan yang ada. Tujuannya adalah memberikan arahan untuk upaya keamanan informasi di masa depan.

Pada aktivitas ini dilakukan peninjauan kembali terhadap informasi-informasi yang ada pada *Security Practices Worksheet* mengenai status *stoplight* untuk masing-masing area, sejauh mana masing-masing area praktik keamanan telah diterapkan di dalam organisasi, serta praktik keamanan apa saja yang telah dilaksanakan dengan baik dan mana yang belum oleh organisasi tersebut. Selanjutnya yang dilakukan adalah memindahkan setiap status *stoplight* yang dimiliki oleh masing-masing area praktik keamanan pada *Security Practices Worksheet* ke area yang telah ditunjukkan pada *Protection Strategy Worksheet*. Kemudian mengembangkan strategi perlindungan yang sesuai untuk setiap area praktik keamanan.

b. S5.2 Memilih Pendekatan Mitigasi

Pendekatan mitigasi adalah bagaimana sebuah organisasi bermaksud untuk mengatasi suatu risiko. Terdapat beberapa pilihan untuk menangani setiap risiko, yaitu menerima (*accept*), mengurangi (*mitigate*), atau menunda (*defer*).

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

- Terima (*accept*) - keputusan yang dibuat untuk tidak mengambil tindakan apapun untuk mengatasi risiko dan menerima konsekuensi jika risiko terjadi. Risiko yang diterima biasanya berdampak rendah pada suatu organisasi.
- Kurangi (*mitigate*) - keputusan yang dibuat untuk mengatasi risiko dengan melaksanakan kegiatan yang dirancang untuk melawan ancaman yang mendasarinya. Risiko yang dimitigasi biasanya memiliki dampak tinggi pada suatu organisasi.
- Tunda (*defer*) - situasi di mana risiko tidak diterima atau dimitigasi. Dampak pada organisasi karena risiko yang ditangguhkan adalah di atas ambang minimal, tetapi tidak begitu besar untuk menjadi prioritas langsung. Risiko yang ditangguhkan diawasi dan dievaluasi kembali di masa depan.

Langkah pertama yang dilakukan dalam aktivitas ini adalah memindahkan informasi yang telah diperoleh dari penilaian masing-masing area praktik keamanan. Informasi status *stoplight* untuk masing-masing *Security Practice Areas* dipindah ke bagian "*Security Practice Areas*" dari setiap *Risk Profile Worksheet* yang dimiliki oleh aset kritis.

Langkah selanjutnya yang dilakukan adalah memilih tiga area praktik keamanan yang akan digunakan sebagai area mitigasi. Area mitigasi merupakan area praktik keamanan yang rencananya akan ditingkatkan guna mengurangi satu atau lebih risiko keamanan organisasi. Jumlah area yang dipilih dapat bergantung pada kebijakan yang dibuat, sehingga memungkinkan untuk memilih lebih dari atau kurang dari tiga area mitigasi. Informasi yang dikumpulkan pada tahapan-tahapan sebelumnya akan membantu dalam menentukan alasan mengapa area tersebut dipilih sebagai area mitigasi. Selanjutnya memilih risiko yang akan dimitigasi, diterima atau dievaluasi kembali di masa yang akan datang.

Pada saat menentukan area yang akan dipilih untuk mitigasi, ada beberapa hal dapat menjadi pertimbangan seperti area praktik keamanan mana yang membutuhkan peningkatan. Dalam hal ini, area praktik keamanan manakah yang apabila dipilih akan mengurangi banyak risiko dari beberapa aset; serta ada atau tidaknya peraturan atau kebijakan yang menjadi pertimbangan dalam memilih area mitigasi.

c. S5.3 Mengembangkan Rencana Mitigasi Risiko

Rencana mitigasi risiko adalah rencana yang dimaksudkan untuk mengurangi risiko pada aset kritis. Rencana mitigasi risiko cenderung menggabungkan kegiatan, atau penanggulangan yang dirancang untuk melawan ancaman terhadap aset.

Ada dua jenis kegiatan mitigasi: aktivitas mitigasi luas dan kegiatan mitigasi terfokus. Aktivitas mitigasi yang luas memicu adanya perubahan pada pendekatan yang digunakan untuk karakteristik area praktik keamanan. Sedangkan kegiatan mitigasi yang terfokus tidak perlu mengubah pendekatan untuk karakteristik area praktik keamanan serta meningkatkan cara pendekatan yang digunakan saat ini untuk karakteristik area praktik keamanan yang sedang

diimplementasikan. Kegiatan mitigasi yang terfokus sering digunakan pada aset tertentu atau terkonsentrasi pada perbaikan khusus.

Rencana mitigasi risiko sering dikaitkan dengan survivabilitas atau daya bertahan suatu perusahaan. Rencana tersebut umumnya dirancang untuk mengurangi risiko yang dapat mencegah organisasi mencapai misinya dengan mengatasi ancaman yang mendasarinya.

Rencana mitigasi risiko terdiri dari unsur-unsur berikut:

- **Kegiatan mitigasi** - mendefinisikan kegiatan yang direkomendasikan untuk diterapkan pada area praktik keamanan.
- **Alasan** - mendokumentasikan alasan dalam memilih setiap kegiatan mitigasi.
- **Tanggung jawab mitigasi** - mengidentifikasi siapa yang harus dilibatkan dalam melaksanakan setiap kegiatan mitigasi.
- **Dukungan tambahan** - mendokumentasikan dukungan tambahan yang diperlukan ketika menerapkan setiap aktivitas.

Langkah yang dilakukan pada aktivitas ini adalah membuat rencana mitigasi untuk setiap area praktik keamanan yang dipilih sebelumnya. Dalam membuat rencana mitigasi tersebut ada beberapa hal yang harus diperhatikan diantaranya memastikan kegiatan mitigasi apa yang akan dapat mengurangi risiko yang mengarah pada area tersebut, serta alasan yang mendasari pemilihan setiap kegiatan mitigasi. Selain itu juga menentukan siapa saja yang akan terlibat dalam melaksanakan setiap kegiatan hingga dukungan tambahan yang diperlukan saat melaksanakan setiap aktivitas seperti dana dan dukungan staf.

d. S5.4 Mengidentifikasi Perubahan terhadap Strategi Perlindungan

Aktivitas selanjutnya adalah mendokumentasikan perubahan yang dilakukan pada strategi perlindungan yang dimiliki oleh organisasi. Kemudian mengidentifikasi apakah aktivitas mitigasi yang dilakukan menunjukkan perubahan pada strategi perlindungan tersebut. Apabila terjadi perubahan, karakteristik mana yang akan terpengaruh dan pengaruh seperti apa yang ditimbulkan. Kemudian catat apabila terjadi perubahan tambahan yang terjadi pada strategi perlindungan.

Strategi perlindungan organisasi mendefinisikan pendekatan yang digunakan oleh organisasi untuk mengaktifkan, memulai, menerapkan, dan menjaga keamanan internalnya, selain itu memberikan arahan untuk upaya keamanan informasi di masa mendatang.

e. S5.5 Mengidentifikasi Langkah Selanjutnya

Membuat serangkaian langkah berikutnya menandai akhir dari OCTAVE-S. Kegiatan ini mengharuskan tim analisis untuk mempertimbangkan apa yang harus dilakukan untuk memfasilitasi pelaksanaan hasil evaluasi. Langkah selanjutnya biasanya membahas empat bidang berikut:

- Sponsor manajemen untuk peningkatan keamanan

Mendefinisikan apa yang harus dilakukan manajemen untuk mendukung pelaksanaan hasil-hasil analisis OCTAVE-S

- Pemantauan implementasi
  Mengidentifikasi apa yang akan dilakukan oleh organisasi untuk menganalisis kemajuan dan memastikan bahwa hasil OCTAVE-S telah diterapkan
- Memperluas evaluasi risiko keamanan informasi saat ini
  Menentukan apakah organisasi perlu memperluas evaluasi OCTAVE-S saat ini untuk menyertakan tambahan aset penting atau area operasional tambahan
- Evaluasi risiko keamanan informasi selanjutnya
  Menentukan kapan organisasi akan melakukan evaluasi OCTAVE-S berikutnya

Langkah berikutnya adalah melakukan peninjauan terhadap informasi dengan mempertimbangkan beberapa hal seperti langkah atau tindakan yang harus dilakukan manajemen untuk mendukung pelaksanaan hasil OCTAVE-S. Setelah itu memastikan apa yang akan dilakukan oleh organisasi untuk mengetahui kemajuan atau hasil dari evaluasi keamanan risiko yang dilakukan, serta memastikan bahwa hasil evaluasi tersebut diimplementasikan.

Selanjutnya mendokumentasikan hasil evaluasi OCTAVE-S secara resmi dengan menyesuaikan pada pedoman dokumentasi yang normal dan biasa digunakan oleh organisasi serta harus disesuaikan untuk memenuhi kebutuhan organisasi. Aktivitas ini akan menandai akhir dari serangkaian proses kerangka kerja OCTAVE-S. Informasi yang dihasilkan akan berfungsi sebagai sumber bahan untuk evaluasi berikutnya dan juga berguna untuk mengetahui rencana dan tindakan yang dilakukan setelah evaluasi.

Dari ketiga tahapan fase tersebut, maka akan didapatkan output atau keluaran dari masing-masing fase seperti yang tertera pada tabel 2.1 berikut:

Tabel 2.6 OCTAVE-S *Outputs*

Fase	Output
Fase 1	• Aset Kritis • Kebutuhan keamanan untuk aset kritis • Ancaman pada aset kritis • Praktik keamanan saat ini • Kerentanan organisasi saat ini
Fase 2	• Komponen utama • Kerentanan teknologi saat ini
Fase 3	• Risiko aset kritis • Pengukuran risiko • Strategi perlindungan • Perencanaan mitigasi risiko

2.7 *Failure Mode and Effect Analysis* (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. Potensi yang teridentifikasi akan diklasifikasikan atau dikelompokkan berdasarkan besarnya potensi kegagalan yang ditimbulkan serta dampak yang dihasilkan terhadap proses. FMEA juga digunakan untuk mengurangi peluang terjadinya kegagalan (Stamatis, 2003).

Menurut Stamatis (1995), FMEA merupakan sebuah metodologi yang dapat digunakan untuk mengevaluasi kegagalan yang mungkin terjadi di dalam sebuah sistem, desain, pelayanan maupun 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*).

FMEA digunakan untuk menganalisa potensi kegagalan atau kesalahan di dalam suatu sistem yang kemudian akan diklasifikasikan menurut besar dan kecilnya potensi kegagalan dan dampak yang dihasilkan terhadap proses. Secara umum, FMEA didefinisikan sebagai suatu teknik yang digunakan untuk mengidentifikasi tiga hal, yaitu:

1. Penyebab kegagalan potensial dari suatu sistem, desain, proses dan pelayanan selama siklus hidupnya.
2. Dampak dari kegagalan.
3. Tingkat kekritisan dampak kegagalan terhadap fungsi dan kerja suatu sistem, desain, proses dan pelayanan.

FMEA dapat memberikan manfaat yang besar dalam membantu proses pengambilan keputusan selama perancangan dan pengembangan dilakukan. Selain itu FMEA juga merupakan sebuah alat yang dapat diandalkan untuk mengurangi kerugian yang dihasilkan dari kegagalan tersebut.

Berikut merupakan langkah-langkah penerapan FMEA:

1. ***Identify components and associated functions***
   Langkah pertama FMEA adalah mengidentifikasi semua komponen yang akan dievaluasi. Kemudian fungsi dari masing-masing komponen akan dijelaskan secara singkat.
2. ***Identify failure modes***
   Mengidentifikasi modus kegagalan potensial untuk setiap komponen. Hal yang harus diperhatikan bahwa mungkin ada beberapa komponen yang memiliki lebih dari satu modus kegagalan.
3. ***Identify effects of the failure modes***
   Mengidentifikasi dampak atau konsekuensi yang dihasilkan dari kegagalan yang terjadi.
4. ***Determine severity of the failure mode***

Menentukan tingkat keparahan (*severity*) dari kegagalan yang terjadi. Tingkat keparahan tersebut biasanya ditentukan dengan nilai.

5. ***Identify cause(s) of the failure mode***
   Melakukan identifikasi terhadap penyebab dari kegagalan yang terjadi.
6. ***Determine probability of occurrence***
   Menentukan atau memperkirakan probabilitas suatu kegagalan dapat terjadi dan seberapa sering kegagalan tersebut terjadi (*occurence*).
7. ***Identify controls***
   Mengidentifikasi kontrol yang ada saat ini untuk mencegah atau mendeteksi penyebab terjadinya kegagalan. Tindakan kontrol juga dapat menghilangkan penyebab atau mengurangi tingkat kegagalan tersebut.
8. ***Determine effectiveness of current controls***
   Menentukan tingkat efektivitas kontrol (*detection*). Penentuan ini berfungsi untuk memperkirakan seberapa baik penyebab atau kegagalan dapat dicegah atau dideteksi.
9. ***Calculate Risk Priority Number (RPN)***
   Menghitung nilai RPN (*risk priority number*). RPN adalah langkah opsional yang dapat digunakan untuk membantu menentukan prioritas dari kegagalan. RPN dihitung dengan mengalikan nilai keparahan (S), probabilitas kejadian (O) dan efektivitas kontrol (D).
10. ***Determine actions to reduce risk of failure mode***
    Langkah terakhir dan merupakan aspek yang paling penting dari FMEA adalah pengambilan tindakan untuk mengurangi risiko kegagalan. FMEA harus ditinjau ulang untuk menentukan di mana tindakan perbaikan harus dilakukan, tindakan apa yang harus dilakukan dan kapan tindakan tersebut dilakukan.

2.7.1 Tujuan *Failure Mode and Effect Analysis* (FMEA)

Berdasarkan pengertian-pengertian yang terlah dijelaskan, FMEA bertujuan untuk:

1. Memprediksi dan mengenali potensi kegagalan yang dapat terjadi dari suatu proses.
2. Memprediksi dan mengevaluasi pengaruh yang ditimbulkan dari kegagalan yang terjadi.
3. Menunjukkan dan memberikan perbaikan terhadap suatu proses maupun sub-sistem melalui daftar prioritas penanganan yang harus didahulukan.
4. Memberikan dan menganalisis tindakan-tindakan perbaikan yang dapat dilakukan untuk mencegah atau mengurangi kemungkinanan terjadinya potensi kegagalan yang akan berpengaruh terhadap suatu sistem maupun proses.
5. Mendokumentasikan keseluruhan proses yang telah dilakukan.

2.7.2 Tahapan *Failure Mode and Effect Analysis* (FMEA)

2.7.2.1 Penentuan Nilai Dampak (*Severity*)

Severity merupakan penilaian yang dilakukan terhadap dampak atau konsekuensi yang dirasa memberikan pengaruh buruk terhadap aset kritis yang diakibatkan oleh kegagalan potensial. *Severity* menilai tingkat keparahan dampak yang dihasilkan. Penilaian nilai dampak atau *severity* dilihat dari seberapa besar intensitas suatu gangguan atau kejadian dapat memberikan pengaruh pada aspek-aspek penting di dalam organisasi. Terdapat tiga aspek yang menjadi fokus pada penilaian dampak, yaitu aspek jadwal, aspek biaya, dan aspek teknis. Penilaian *severity* membantu mengukur dampak atau konsekuensi dengan memberikan kriteria penilaian seperti yang terdapat pada tabel dibawah ini:

Tabel 2.2 Kriteria Nilai Dampak (*Severity*)

Ranking	Tingkat Intensitas Dampak	Dampak Yang Dihasilkan
1	Tidak Ada Dampak	Tanpa disadari dan tidak memberikan pengaruh pada kinerja
2	Sangat Ringan	Tanpa disadari namun mengakibatkan gangguan kecil pada kinerja
3	Ringan	Menyebabkan gangguan kecil yang dapat diatasi tanpa menghilangkan sesuatu apapun
4	Minor	Menyebabkan sedikit kerugian
5	Moderat	Menyebabkan penurunan terhadap kinerja serta menimbulkan keluhan
6	Signifikan	Menghasilkan kerugian berupa kerusakan parsial secara moderat
7	Major	Menimbulkan ketidakpuasan pelanggan secara ekstrim
8	Ekstrim	Mengubah produk atau jasa yang dihasilkan menjadi tidak layak untuk digunakan
9	Serius	Aktivitas illegal
10	Berbahaya	Melukai karyawan atau pelanggan

2.7.2.2 Penentuan Nilai Probabilitas (*Occurence*)

Occurence merupakan sebuah penilaian yang dilakukan terhadap probabilitas suatu kegagalan dapat terjadi dan seberapa sering terjadinya gangguan yang dapat menimbulkan kegagalan. Penilaian *occurence* membantu

mengukur probabilitas dengan memberikan kriteria penilaian seperti yang terdapat pada tabel dibawah ini:

Tabel 2.3 Kriteria Nilai Probabilitas (*Occurence*)

Ranking	Tingkat Kemungkinan Kegagalan	Kemungkinan Terjadi
1	Remote: Tidak pernah terjadi kegagalan	Satu kali dalam 6-50 tahun
2	Very Low: Kemungkinan terjadinya kegagalan sangat jarang dan relatif kecil	Satu kali dalam 3-6 tahun
3	Low: Kemungkinan terjadinya kegagalan relatif kecil	Satu kali dalam 1-3 tahun
4	Moderate Low: Kegagalan jarang terjadi	Satu kali dalam setahun
5	Moderate: Kegagalan hanya sesekali terjadi	Satu kali dalam 6 bulan
6	Moderately High: Kegagalan terjadi pada saat tertentu	Satu kali dalam 3 bulan
7	High: Kegagalan sering terjadi	Satu kali dalam sebulan
8	High: Kegagalan terjadi berulang kali	Satu kali dalam seminggu
9	Very High: Kegagalan selalu terjadi	Satu kali setiap 3-4 hari
10	Very High: Kegagalan hampir atau tidak dapat dihindari	Lebih dari satu kali di setiap hari

2.7.2.3 Penentuan Nilai Deteksi (*Detection*)

Detection merupakan sebuah penilaian yang dilakukan terhadap kemampuan organisasi atau perusahaan dalam melakukan pengendalian atau kontrol terhadap kegagalan yang dapat terjadi. Penilaian *detection* membantu mengukur kemampuan deteksi dan kontrol terhadap risiko dengan memberikan kriteria penilaian seperti yang terdapat pada tabel dibawah ini:

Tabel 2.4 Kriteria Nilai Deteksi (*Detection*)

Ranking	Tingkat Deteksi atau Kontrol	Kriteria Deteksi
1	Sangat Baik	Metode deteksi hampir dipastikan dapat mendeteksi risiko dengan waktu yang cukup untuk melaksanakan rencana kontingensi
2	Sangat Tinggi	Metode deteksi sangat efektif untuk dapat mendeteksi risiko dengan waktu yang cukup untuk melaksanakan rencana kontingensi
3	Tinggi	Metode deteksi memiliki kemungkinan yang tinggi untuk dapat mendeteksi adanya risiko kegagalan
4	Cukup Tinggi	Metode deteksi memiliki kemungkinan yang cukup tinggi untuk dapat mendeteksi adanya risiko kegagalan
5	Sedang	Metode deteksi memiliki kemungkinan sedang atau rata-rata dalam mendeteksi risiko
6	Rendah	Metode deteksi memiliki kemampuan efektifitas yang rendah untuk mendeteksi risiko
7	Sangat Rendah	Metode deteksi memiliki kemampuan yang tidak handal dalam melakukan deteksi terhadap risiko dengan tepat waktu

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Ranking	Tingkat Deteksi atau Kontrol	Kriteria Deteksi
8	Kecil	Metode deteksi memiliki kemampuan yang tidak terbukti untuk mendeteksi tepat waktu
9	Sangat Kecil	Metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi
10	Tidak Efektif	Tidak ada metode deteksi atau penanganan yang dilakukan

2.7.2.4 Penentuan Tingkat Prioritas Risiko (*Risk Priority Number*)

Risk Priority Number (RPN) merupakan sebuah produk yang dihasilkan dari perhitungan matematis antara nilai dampak (*severity*) yang menunjukkan tingkat keseriusan dampak yang dihasilkan dari risiko, nilai probabilitas (*occurence*) yang menunjukkan tingkat kemungkinan terjadinya risiko dan nilai deteksi (*detection*) yang menunjukkan tingkat kemampuan dalam mendeteksi potensi terjadinya kegagalan. 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. Berdasarkan FMEA, tingkat risiko diklasifikasikan atau dibagi menjadi beberapa tingkatan seperti dibawah ini:

Tabel 2.5 Tingkat Risiko

Tingkat Risiko	Skala Nilai RPN
Very High	> 200
High	< 200
Medium	< 120
Low	< 80
Very Low	< 20

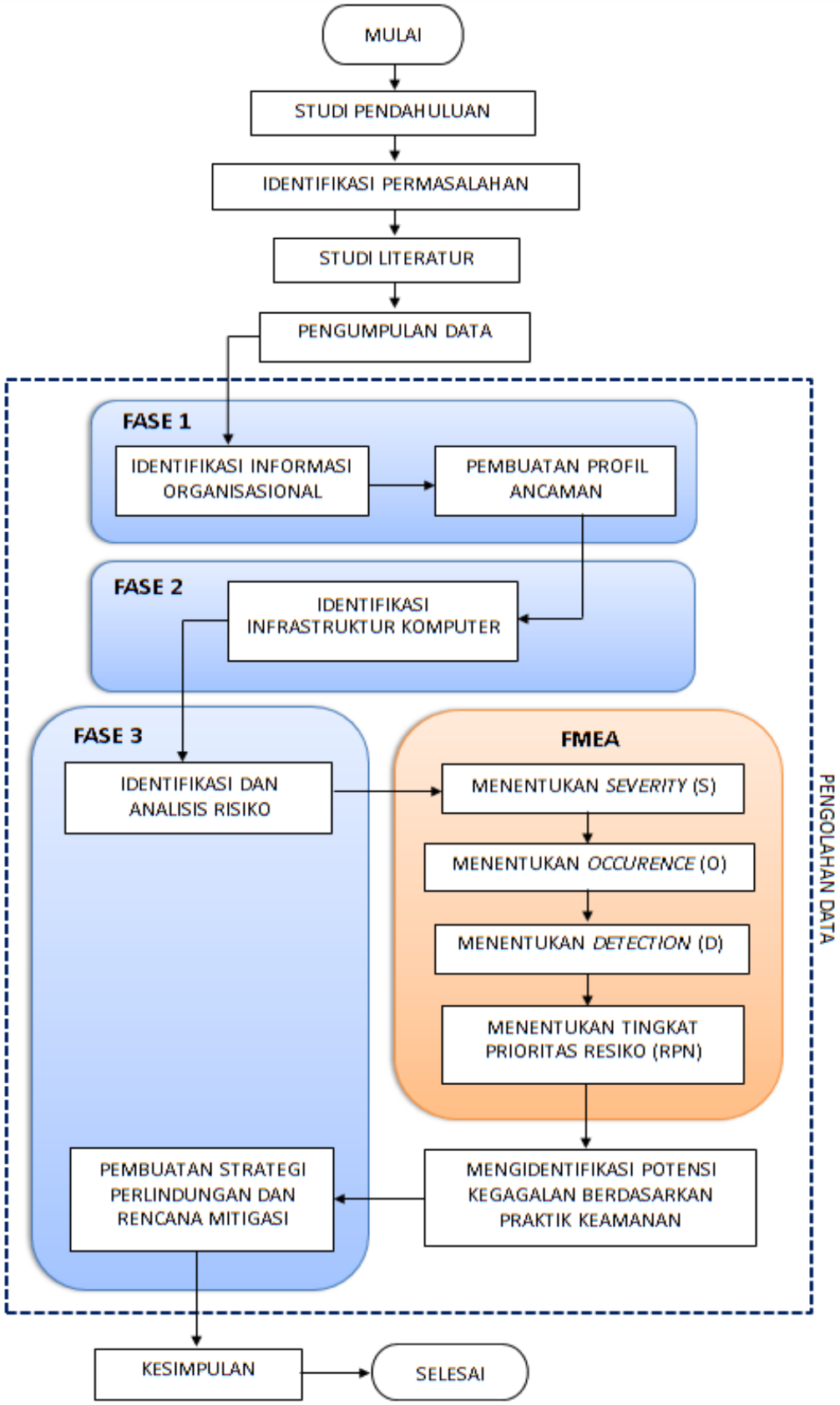
Skala RPN digunakan untuk menentukan tingkat risiko yang kemudian akan menjadi acuan untuk menilai risiko mana yang memiliki tingkatan yang paling tinggi. Perusahaan atau organisasi memerlukan tindakan antisipasi, mitigasi dan

strategi terhadap risiko yang memiliki tingkatan level paling tinggi. Hal ini berguna untuk menjaga keberlangsungan operasional bisnis saat gangguan tersebut terjadi.

Pada dasarnya desain pada FMEA ditujukan untuk mengurangi tingkat RPN dengan cara yang lebih spesifik. Cara spesifik tersebut diantaranya adalah mengurangi tingkat nilai dampak, nilai probabilitas dan nilai deteksi yang dimiliki oleh masing-masing risiko.

BAB 3 METODOLOGI PENELITIAN

Dalam bab ini akan dijelaskan tentang langkah-langkah kerangka kerja yang harus dilakukan dalam melaksanakan sebuah penelitian. Penelitian dilakukan dengan menggunakan pendekatan kualitatif. Pengumpulan data kualitatif dilakukan dengan menggunakan wawancara dan observasi pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Di bawah ini adalah Gambar 3.1, dimana merupakan *flowchart* dari kerangka kerja dalam metodologi penelitian.



Gambar 3.1 Kerangka Kerja Penelitian

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

3.1 Identifikasi Permasalahan

Dalam tahapan ini, akan dilakukan identifikasi terhadap permasalahan yang ada mengenai pentingnya manajemen risiko teknologi informasi pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer.

Proses identifikasi permasalahan ini didukung dengan adanya studi literatur yang dilakukan untuk memperkuat data dan sebagai referensi untuk memberikan aspek integritas pada penelitian ini. Tahapan ini akan menghasilkan rumusan permasalahan serta latar belakang penelitian yang dijadikan sebagai bahan dasar untuk memulai penelitian ini.

3.2 Studi Literatur

Studi literatur dilakukan terhadap sumber referensi yang berkaitan dengan topik penelitian untuk mendukung penyelesaian masalah dan pencapaian tujuan penelitian yang diharapkan. Studi literatur dilakukan pada referensi seperti studi pustaka tentang Teknologi Informasi, Manajemen Risiko Teknologi Informasi, dan kerangka kerja OCTAVE-S. Referensi yang akan digunakan dapat diambil dari buku, jurnal, laporan penelitian yang telah lebih dulu dilakukan maupun dengan melakukan pencarian artikel yang ada di internet. Dalam penelitian ini, studi literatur tidak hanya akan dilakukan pada tahapan awal penelitian, namun juga pada setiap tahapan metodologi penelitian yang ada. Studi literatur juga dilakukan terhadap penelitian-penelitian tentang manajemen risiko teknologi informasi yang pernah dilakukan sebelumnya.

3.3 Pengumpulan Data

Pada tahap ini, terdapat beberapa langkah yang dilakukan untuk melakukan pengumpulan dan pengolahan data diantaranya dengan menggunakan teknik wawancara dan observasi. Kemudian akan dilakukan proses verifikasi kepada pihak organisasi untuk memastikan kebenaran data dan informasi, sehingga diperoleh data dan informasi yang dapat dipertanggung jawabkan.

3.3.1 Wawancara

Tahap wawancara akan dilakukan kepada narasumber terkait yang memiliki pengetahuan tentang teknologi informasi yang ada pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Wawancara akan dilakukan untuk dapat melakukan pengumpulan data dan informasi yang dibutuhkan pada penelitian ini. Pada metode wawancara akan digali informasi mengenai kondisi terkini dari organisasi, penerapan teknologi informasi pada organisasi, ancaman risiko beserta dampak yang dihasilkan pada organisasi. Proses pengumpulan data disesuaikan dengan standar acuan yang terkait, yaitu OCTAVE-S.

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

3.3.2 Observasi

Tahap observasi dilakukan pada saat mengumpulkan data untuk menganalisis risiko. Di mana, pada tahapan identifikasi risiko, diperlukan pengamatan untuk bisa mengidentifikasikan dengan tepat, risiko teknologi informasi yang mungkin muncul pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Pengamatan juga dilakukan terhadap kinerja dan aktivitas yang ada pada Unit PSIK Fakultas Ilmu Komputer untuk menggali informasi mengenai risiko yang potensial.

3.4 Pengolahan Data

Berdasarkan informasi kondisi terkini dari organisasi, risiko dan dampak potensial pada organisasi, maka proses selanjutnya adalah mengolah data dan informasi yang telah dimiliki.

3.4.1 Identifikasi Informasi Organisasional

Pada tahapan ini, terdapat tiga aktivitas yang akan dilakukan untuk mengidentifikasi informasi-informasi yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Aktivitas pertama yang akan dilakukan adalah menerapkan kriteria dampak yang digunakan untuk mengevaluasi efek dari keberadaan ancaman risiko terhadap misi dan tujuan bisnis yang dimiliki oleh organisasi maupun perusahaan. Kriteria yang dibuat akan digunakan untuk mengukur seberapa besar dampak yang ditimbulkan dengan menetapkan *range* tinggi, sedang dan rendah untuk masing-masing kriteria. Beberapa kriteria dampak yang ditetapkan oleh organisasi diantara lain adalah

- Reputasi atau Kepercayaan Pelanggan
- Keuangan
- Produktivitas
- Keamanan/keselamatan dan Kesehatan
- Denda atau Hukuman

Aktivitas berikutnya adalah mengidentifikasi aset-aset teknologi informasi yang dimiliki oleh organisasi. Aset-aset yang dimiliki dapat berupa sistem, informasi, layanan dan aplikasi yang dibutuhkan oleh organisasi tersebut untuk menunjang tugas dan fungsinya serta aset manusia atau orang-orang yang ada di dalam organisasi. Orang-orang ini adalah mereka yang memiliki kemampuan yang penting bagi organisasi sehingga posisi mereka sulit untuk digantikan.

Dan aktivitas yang terakhir adalah melakukan evaluasi terhadap praktik keamanan yang telah dilaksanakan oleh organisasi. Proses evaluasi dilakukan dengan melakukan peninjauan pernyataan di setiap area praktik keamanan pada *Security Practices Worksheet*, kemudian memberikan penilaian dengan kriteria *Very Much, Somewhat* dan *Not At All* untuk masing-masing pernyataan yang tertera. Setelah melakukan penilaian pada masing-masing pernyataan, selanjutnya menetapkan status *stoplight* untuk area praktik keamanan yang dievaluasi dengan kriteria hijau, kuning dan merah. Status *stoplight* tersebut

akan mencerminkan seberapa baik praktik keamanan yang telah diterapkan oleh organisasi pada setiap area.

3.4.2 Pembuatan Profil Ancaman

Pada tahapan ini, terdapat tiga aktivitas yang akan dilakukan untuk membuat profil ancaman. Aktivitas pertama adalah memilih aset kritis dari keseluruhan aset teknologi informasi yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Pemilihan dilakukan dengan mempertimbangkan aset mana yang berisiko menimbulkan dampak kerugian yang besar pada organisasi apabila aset tersebut terancam. Selanjutnya mengidentifikasi siapa yang bertanggung jawab terhadap aset tersebut, serta apakah ada aset lain yang memiliki keterkaitan dengan aset penting yang dipilih.

Aktivitas berikutnya adalah mengidentifikasi kebutuhan untuk masing-masing aset kritis yang telah teridentifikasi. Kebutuhan keamanan tersebut berfokus pada kebutuhan apa yang seharusnya ada untuk suatu aset, bukan apa yang sedang diterapkan saat ini. Kemudian aktivitas yang terakhir adalah mengidentifikasi ancaman risiko untuk masing-masing aset kritis tersebut.

Pada aktivitas tersebut terdapat beberapa *worksheet* yang dapat digunakan untuk mengidentifikasi risiko dari berbagai jalur atau sumber, seperti ancaman risiko yang dapat berasal dari akses yang dilakukan manusia baik melalui jalur jaringan maupun fisik, masalah pada sistem hingga masalah lainnya seperti bencana alam dan lain sebagainya. Selanjutnya mengidentifikasi seberapa sering risiko tersebut terjadi di masa lalu.

3.4.3 Identifikasi Infrastruktur Komputer

Pada tahapan ini, terdapat dua aktivitas yang akan dilakukan untuk mengidentifikasi infrastruktur komputer yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Aktivitas pertama yang dilakukan adalah memeriksa jalur akses yang digunakan dengan menentukan sistem yang memiliki keterkaitan paling erat dengan aset kritis. Kemudian mengidentifikasi komponen-komponen apa saja yang menjadi bagian dari sistem tersebut (*server, on-site workstation*), mengidentifikasi bagaimana informasi dan aplikasi dari sistem tersebut ditransmisikan kepada orang-orang yang mengakses sistem tersebut (jaringan internal, jaringan eksternal).

Selanjutnya mengidentifikasi komponen apa saja yang digunakan oleh orang-orang untuk dapat mengakses sistem tersebut. Jenis komponen apa saja yang digunakan untuk dapat mengakses sistem, seperti *on-site workstation*, laptop, komponen *wireless*, dan lain-lain. Langkah berikutnya adalah menentukan lokasi penyimpanan data atau informasi yang dimiliki oleh sistem (media penyimpanan internal, eksternal). Langkah terakhir pada aktivitas ini adalah mengidentifikasi sistem lain apa saja yang juga ikut mengakses informasi, layanan, atau aplikasi dari sistem tersebut, serta komponen apa saja yang dapat digunakan untuk melakukan akses.

Aktivitas berikutnya adalah menganalisis kembali komponen-komponen apa saja yang memiliki keterkaitan dengan aset kritis dengan melakukan

identifikasi terhadap aset-aset yang berkaitan dengan komponen tersebut. Pada aktivitas ini juga akan dilakukan identifikasi terhadap siapa saja yang bertanggung jawab dalam memelihara atau *maintenance* serta bertanggung jawab terhadap keamanan untuk masing-masing komponen.

3.4.4 Identifikasi dan Analisis Risiko

Pada tahapan ini, terdapat tiga aktivitas yang akan dilakukan untuk mengidentifikasi dan menganalisis risiko. Aktivitas pertama yang dilakukan adalah mengevaluasi dampak potensial dari ancaman risiko yang terjadi pada aset kritis dengan meninjau ulang informasi terkait aset kritis, aktor yang berpotensi untuk menimbulkan ancaman, motif yang dimiliki, catatan risiko yang terjadi di masa lalu, kebutuhan keamanan masing-masing aset kritis, serta dampak potensial yang akan diterima oleh organisasi dan tujuan bisnis organisasi.

Aktivitas berikutnya adalah menentukan ukuran probabilitas terjadinya risiko berdasarkan seberapa sering ancaman tersebut terjadi di masa lalu. Kemudian setelah melakukan evaluasi terhadap informasi-informasi diatas, aktivitas terakhir yang akan dilakukan adalah menentukan probabilitas ancaman risiko akan terjadi di masa yang akan datang.

3.4.5 Menentukan Tingkat Keparahan Dampak (*Severity*)

Pada tahapan ini, dilakukan penilaian terhadap dampak atau konsekuensi yang dirasa memberikan pengaruh buruk terhadap aset kritis yang diakibatkan oleh kegagalan potensial. Penilaian dilakukan untuk melihat seberapa tingkat keparahan dampak yang dihasilkan.

3.4.6 Menentukan Tingkat Probabilitas Kejadian (*Occurence*)

Pada tahapan ini, dilakukan penilaian terhadap probabilitas terjadinya suatu kegagalan dan seberapa sering gangguan yang dapat menimbulkan kegagalan tersebut terjadi.

3.4.7 Menentukan Tingkat Kemampuan Deteksi (*Detection*)

Pada tahapan ini, dilakukan penilaian terhadap kemampuan organisasi atau perusahaan dalam melakukan pengendalian atau kontrol terhadap kegagalan yang dapat terjadi.

3.4.8 Menentukan Tingkat Prioritas Risiko (RPN)

Pada tahapan ini, dilakukan perhitungan tingkat prioritas risiko (RPN) yang dihasilkan antara nilai dampak (*severity*) yang menunjukkan tingkat keseriusan dampak yang dihasilkan dari risiko, nilai probabilitas (*occurence*) yang menunjukkan tingkat kemungkinan terjadinya risiko dan nilai deteksi (*detection*) yang menunjukkan tingkat kemampuan dalam mendeteksi potensi terjadinya kegagalan. Dari hasil perhitungan tersebut maka akan diperoleh hasil yang digunakan untuk menentukan tingkat risiko.

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

3.4.9 Mengidentifikasi Potensi Kegagalan Berdasarkan Praktik Keamanan

Pada tahapan ini, dilakukan penggabungan antara kedua hasil yang diperoleh dari tahapan-tahapan sebelumnya serta melakukan analisis. 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.

Analisis ini bertujuan untuk mengetahui apakah setiap potensi kegagalan atau risiko yang teridentifikasi dengan menggunakan kerangka kerja OCTAVE-S serta kemudian dinilai dan diukur dengan menggunakan metode FMEA akan sesuai dengan masing-masing pernyataan praktik keamanan yang terdapat dalam kerangka kerja OCTAVE-S itu sendiri. Selain itu, analisis ini akan membantu untuk mengetahui apakah hasil penilaian atau pengukuran tingkat prioritas risiko dengan menggunakan metode FMEA akan sesuai dengan hasil penilaian praktik keamanan yang ada di dalam kerangka kerja OCTAVE-S.

3.4.10 Pembuatan Strategi Perlindungan dan Rencana Mitigasi

Pada tahapan ini, terdapat lima aktivitas yang akan dilakukan untuk mengembangkan strategi perlindungan dan rencana mitigasi pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Aktivitas pertama yang dilakukan adalah menjelaskan strategi perlindungan yang telah dilakukan oleh organisasi saat ini. Hal tersebut dilakukan dengan melihat kembali seluruh informasi mengenai penilaian status *stoplight* yang dilakukan pada masing-masing area praktik keamanan, sejauh mana masing-masing area praktik keamanan telah diterapkan di dalam organisasi, serta praktik keamanan apa saja yang telah dilaksanakan dengan baik dan mana yang belum oleh Unit PSIK Fakultas Ilmu Komputer.

Berdasarkan evaluasi dan penilaian yang telah dilakukan sebelumnya dengan menggunakan status *stoplight,* selanjutnya menentukan area praktik keamanan yang akan dipilih sebagai area yang dimitigasi. Pemilihan area mitigasi ini bergantung pada kebijakan yang dibuat berdasarkan semua informasi seperti informasi mengenai aset kritis, profil ancaman, praktik keamanan serta informasi mengenai infrastruktur komputer yang telah dikumpulkan sebelumnya. Penentuan area praktik kemanan yang dimitigasi juga mempertimbangkan area mana yang membutuhkan peningkatan dan perbaikan sehingga dapat mengurangi potensi munculnya ancaman risiko terhadap aset kritis.

Selanjutnya membuat rencana mitigasi untuk setiap area praktik keamanan yang telah dipilih sebelumnya. Rencana mitigasi yang dibuat harus dipastikan dapat mengurangi risiko yang mengarah pada area tersebut. Kemudian menentukan siapa saja yang harus terlibat serta dukungan apa saja yang diperlukan dalam melaksanakan setiap kegiatan mitigasi. Kemudian setelah itu memastikan apa yang akan dilakukan oleh Unit PSIK Fakultas Ilmu Komputer

untuk mengetahui kemajuan atau hasil dari evaluasi keamanan risiko yang dilakukan, serta memastikan bahwa hasil evaluasi tersebut diimplementasikan.

3.5 Kesimpulan

Setelah semua tahap penelitian mulai dari studi literatur hingga pembuatan strategi perlindungan dan rencana mitigasi telah selesai dilaksanakan, maka tahap akhir yang perlu dilakukan adalah pengambilan kesimpulan. Kesimpulan yang diambil didasarkan pada hasil analisis data yang telah dilakukan sebelumnya. Selain melakukan pengambilan kesimpulan, selanjutnya akan diberikan saran untuk melakukan tahap manajemen risiko lebih lanjut untuk mengatasi risiko yang ada serta memberi pertimbangan yang berguna untuk penelitian lebih lanjut.

BAB 4 HASIL

4.1 Persiapan Pengumpulan Data

Pada bagian ini akan menjelaskan mengenai tahapan persiapan pengumpulan data dan informasi yang nantinya akan diolah untuk dapat menjawab rumusan masalah. Terdapat beberapa teknik yang digunakan dalam mengumpulkan data dan informasi, antara lain adalah *interview* atau wawancara dan observasi. Pendekatan yang digunakan untuk melakukan pengumpulan data dan informasi yang berhubungan dengan manajemen risiko sistem informasi adalah kerangka kerja OCTAVE-S.

4.1.1 Wawancara

Proses wawancara akan dilakukan pada Ketua Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer serta dua divisi yang terdapat pada PSIK yaitu, Divisi Infrastruktur dan Jaringan serta Divisi Pengembangan Sistem Informasi. Diharapkan setelah melakukan wawancara akan didapatkan informasi terkait risiko TI yang dihadapi oleh perusahaan.

Tabel 4.1 Ketentuan Wawancara

Nama Proses	Pengumpulan Data dan Informasi
Teknik Wawancara	*Interview*/Wawancara Teknik wawancara yang akan digunakan adalah dengan metode tanya jawab langsung dengan narasumber. Wawancara akan dilakukan secara terstruktur, dimana peneliti telah menyiapkan pertanyaan-pertanyaan yang dibutuhkan terlebih dahulu. Pertanyaan-pertanyaan yang digunakan menyesuaikan dengan format yang terdapat pada *handbook* OCTAVE-S.
Objek	Kondisi terkini dari organisasi, aset teknologi informasi, risiko dan dampak yang ditimbulkan bagi organisasi.
Kebutuhan	1. *Interview Protocol* 2. Alat perekam (*handphone*) 3. Alat tulis 4. Laptop
Tahapan Pelaksaan	Tahapan dalam melakukan wawancara adalah sebagai berikut: - Menetapkan tujuan dan jumlah wawancara - Menentukan narasumber - Membuat *interview protocol* - Memulai proses wawancara - Mendokumentasikan hasil wawancara

4.1.1.1 Profil Narasumber Wawancara

Sebelum melakukan wawancara, peneliti terlebih dahulu harus menentukan narasumber. Narasumber yang dipilih tentu saja harus sesuai dengan tujuan wawancara serta berada dalam kapasitas objek wawancara. Hal ini bertujuan agar narasumber dapat memberikan informasi yang valid dan sesuai serta relevan dengan cakupan wawancara itu sendiri. Berikut merupakan profil narasumber yang akan diwawancara dalam penelitian ini:

Tabel 4.2 Profil Narasumber

Nama	Jabatan
Denny Sagita, S.Kom, M.Kom	Ketua Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer
Ivan Yulfrian, S.Kom	Koordinator Divisi Infrastruktur Data dan Jaringan Unit PSIK Fakultas Ilmu Komputer
Dwi Saputro Nugroho, S.Kom	Staff Divisi Pengembangan Sistem Informasi Unit PSIK Fakultas Ilmu Komputer

Penentuan tersebut didasarkan pada jenis informasi yang ingin digali dari narasumber berdasarkan kapasitas mereka. Bapak Denny Sagita dipilih sebagai narasumber untuk penggalian informasi organisasional meliputi praktik keamanan yang telah diterapkan oleh organisasi, identifikasi aset teknologi informasi hingga kebutuhan keamanan untuk masing-masing aset kritis yang dimiliki oleh organisasi. Posisi Bapak Denny sebagai Ketua Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer dinilai sesuai dengan jenis informasi yang akan digali karena beliau merupakan penanggung jawab utama dari seluruh proses bisnis yang ada pada Unit PSIK Fakultas Ilmu Komputer.

Selanjutnya Bapak Dwi Saputro Nugroho dan Bapak Ivan Yulfrian dipilih sebagai narasumber untuk melakukan identifikasi risiko terhadap masing-masing aset kritis meliputi identifikasi terhadap aset teknologi informasi, ancaman risiko pada aset kritis, dan dampak yang dihasilkan bagi organisasi. Dari hasil identifikasi telah didapatkan bahwa Unit PSIK Fakultas Ilmu Komputer memiliki dua aset teknologi informasi yang dinilai kritis, yaitu aplikasi FILKOM Apps serta Infrastruktur Data dan Jaringan. Seperti yang diketahui Bapak Dwy merupakan staff Unit PSIK Divisi Pengembangan Sistem Informasi sedangkan Bapak Ivan merupakan staff Unit PSIK Divisi Infrastruktur dan Jaringan. Mereka dinilai sesuai menjadi narasumber informasi untuk masing-masing aset kritis yang teridentifikasi, yaitu Bapak Dwy pada aplikasi FILKOM Apps dan Bapak Ivan pada Infrastruktur dan Jaringan.

Selain itu mereka juga dinilai sesuai untuk menjadi narasumber penggalian informasi mengenai keterkaitan sistem lain dan komponen-komponen teknologi informasi dengan aset kritis, serta jalur akses yang dapat digunakan oleh orang-orang atau pengguna untuk mengakses aset tenologi informasi pada organisasi.

4.1.1.2 Jumlah dan Tujuan Wawancara

Sebelum melakukan wawancara, terlebih dahulu ditetapkan tujuan dari masing-masing wawancara yang akan dilakukan. Hal ini bertujuan agar nantinya proses wawancara dan pengambilan informasi dapat sesuai dengan tujuan penelitian dan peneliti mendapatkan data dan informasi yang dibutuhkan.

Tabel 4.3 Jumlah dan Tujuan Wawancara

No.	Narasumber	Tujuan Wawancara
1.	Denny Sagita, S.Kom, M.Kom	Wawancara dilakukan untuk mengetahui kondisi terkini dari organisasi, penerapan teknologi informasi yang ada pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Selain itu melakukan identifikasi terhadap aset kritis TI, praktik keamanan TI yang telah diterapkan, kebutuhan keamanan, serta dampak yang diterima apabila terjadi gangguan.
2.	Ivan Yulfrian, S.Kom	Wawancara dilakukan untuk mengidentifikasi lebih jauh mengenai aset kritis serta risiko TI yang terdapat pada infrastruktur data dan jaringan milik PSIK. Selain itu juga melakukan identifikasi terhadap kebutuhan keamanan, keamanan TI yang telah diterapkan, identifikasi ancaman risiko, serta dampak yang diterima apabila terjadi gangguan.
3.	Dwi Saputro Nugroho, S.Kom	Wawancara dilakukan untuk mengidentifikasi lebih jauh mengenai aset kritis serta risiko TI yang terdapat pada sistem dan layanan milik PSIK. Selain itu juga melakukan identifikasi terhadap kebutuhan keamanan, keamanan TI yang telah diterapkan, identifikasi ancaman risiko, kelemahan organisasi serta dampak yang diterima apabila terjadi gangguan.

4.1.1.3 Daftar Pertanyaan Wawancara (*Interview Protocol*)

Pembuatan *interview protocol* didasarkan pada lembar kerja yang telah disediakan oleh OCTAVE-S. Berikut merupakan daftar pertanyaan yang tercantum pada *interview protocol.*

Tabel 4.4 Daftar Pertanyaan Wawancara

No.	Tujuan Pertanyaan	Standar Acuan Terkait	Narasumber	Detail Pertanyaan
1.	Wawancara dilakukan untuk mengetahui dan mendapatkan informasi organisasional PSIK. Hal tersebut dilakukan dengan melakukan identifikasi terhadap praktik keamanan teknologi informasi yang telah diterapkan, aset teknologi informasi dan kebutuhan keamanan untuk aset kritis.	**OCTAVE-S** Fase 1 - Membangun Profil Ancaman Berbasis Aset	Denny Sagita	• Menetapkan kriteria dampak yang terjadi. • Mengetahui dan menilai jenis dampak yang terjadi pada PSIK apabila terjadi ancaman risiko • Mengetahui praktik keamanan yang telah diterapkan • Mengidentifikasi aset teknologi informasi yang digunakan untuk menunjang proses bisnis organisasi • Mengidentifikasi aset kritis organisasi • Mengidentifikasi kebutuhan keamanan untuk aset kritis

No.	Tujuan Pertanyaan	Standar Acuan Terkait	Narasumber	Detail Pertanyaan
2.	Wawancara dilakukan untuk melakukan identifikasi risiko. Hal tersebut dilakukan dengan melakukan identifikasi terhadap aset teknologi informasi, ancaman risiko pada aset kritis, dan dampak yang dihasilkan bagi organisasi.	**OCTAVE-S** Fase 1 - Membangun Profil Ancaman Berbasis Aset	Dwi Saputro Nugroho dan Ivan Yulfrian	• Mengidentifikasi aset teknologi informasi yang digunakan untuk menunjang proses bisnis organisasi • Mengidentifikasi orang-orang yang bertanggung jawab terhadap aset teknologi informasi. • Mengidentifikasi kebutuhan keamanan teknologi informasi organisasi • Mengidentifikasi ancaman risiko yang pernah terjadi pada aset teknologi informasi organisasi • Mengidentifikasi ancaman risiko yang mungkin terjadi pada aset teknologi informasi organisasi • Mengidentifikasi aktor yang berpotensi untuk menimbulkan ancaman risiko pada aset kritis
3.	Wawancara dilakukan untuk melakukan identifikasi terhadap infrastruktur teknologi informasi yang dimiliki oleh organisasi.	**OCTAVE-S** Fase 2 – Mengidentifikasi Kerentanan Infrastruktur	Dwi Saputro Nugroho dan Ivan Yulfrian	• Sistem yang memiliki keterkaitan erat dengan aset teknologi informasi • Komponen-komponen yang menjadi bagian dari aset teknologi informasi • Jalur akses yang digunakan untuk mengakses aset teknologi informasi

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

4.2 Pengolahan Data dan Informasi

Proses berikutnya adalah melakukan pengolahan terhadap data dan informasi yang telah dikumpulkan sebelumnya. Data-data yang telah didapatkan dan dikumpulkan dari Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer kemudian diolah sesuai dengan langkah-langkah yang terdapat pada kerangka kerja OCTAVE-S. Berikut merupakan hasil pengolahan data yang telah dilakukan:

4.2.1 Fase 1*:* Membangun Profil Ancaman Berbasis Asets.

4.2.1.1 Proses 1 - Identifikasi Informasi Organisasi

1. Kriteria Evaluasi Dampak

Tabel 4.5 Kriteria Evaluasi Dampak

Jenis Dampak	Rendah (*Low*)	Sedang (*Medium*)	Tinggi (*High*)
Reputation **(Reputasi)**	Reputasi sedikit terpengaruh, tidak perlu usaha tertentu untuk memperbaiki. Jumlah pelanggan hilang kurang dari 10 % karena hilangnya rasa percaya pelanggan.	Reputasi terganggu, perlu usaha dan biaya untuk memperbaikinya. Jumlah pelanggan hilang kurang antara 10 % - 30 % karena hilangnya rasa percaya pelanggan.	Reputasi hancur. Jumlah pelanggan hilang lebih dari 30 % karena hilangnya rasa percaya pelanggan
Financial **(Keuangan)**	Biaya operational tahunan meningkat kurang dari 2 %. Hilang pendapatan kurang dari 5 %.	Biaya operational tahunan meningkat antara 2 % - 15 %. Hilang pendapatan antara 5 % - 20 %.	Biaya operational tahunan meningkat lebih dari 15 %. Hilang pendapatan lebih dari 20 %.
Productivity **(Produktivitas)**	Jam kerja staff meningkat kurang dari 10 % dalam 1 hingga 2 hari	Jam kerja staff meningkat antara 10 % - 30 % dalam 2 hari	Jam kerja staff meningkat lebih dari 30 % dalam 2 hari
Safety **(Keamanan)**	*Safety questioned* (keamanan dipertanyakan)	*Safety affected* (keamanan terpengaruh)	*Safety violated* (melanggar keamanan)

Jenis Dampak	Rendah (*Low*)	Sedang (*Medium*)	Tinggi (*High*)
***Health* (Kesehatan)**	Minimal, masalah kesehatan ringan yang dapat segera ditangani dengan pemulihan dalam waktu empat hari. Tidak ada kerugian atau ancaman signifikan terhadap kehidupan pelanggan atau karyawan.	Kesehatan pelanggan atau karyawan melemah untuk sementara dan mampu dipulihkan. Kehidupan pelanggan atau karyawan terancam, tetapi akan pulih setelah menerima perawatan medis.	Kehilangan kehidupan pelanggan atau karyawan. Kerusakan permanen terhadap aspek-aspek penting dari kesehatan pelanggan atau karyawan.
***Fines* (Denda)**	Menghasilkan denda kurang dari Rp 50.000.000,00	Menghasilkan denda antara Rp 50.000.000,00 - Rp 100.000.000,00	Menghasilkan denda lebih dari Rp 100.000.000,00

Berdasarkan wawancara yang telah dilakukan dilihat dari segi reputasi, unit Pengelola Sistem Informasi dan Kehumasan (PSIK) memiliki reputasi yang baik. Hal ini terbukti dengan sedikitnya laporan mengenai keluhan terhadap sistem dan layanan yang disediakan oleh PSIK. Sedangkan mengenai jumlah pelanggan atau pengguna layanan, PSIK tidak pernah mengalami pengurangan atau penurunan jumlah pengguna layanan karena sejauh ini belum ada sistem lain yang mampu menjadi alternatif untuk menggantikan tugas dan fungsi dari sistem yang dibuat oleh PSIK.

Kemudian dari segi keuangan, PSIK pernah mengalami kerugian yang cukup besar akibat risiko petir pada tahun 2014. Hal tersebut menyebabkan beberapa infrastruktur seperti *router* dan *access point* mengalami kerusakan sehingga PSIK mengalami kerugian kurang lebih sebesar Rp 300.000.000,00. Sedangkan untuk risiko kecil hingga sedang PSIK belum pernah mengalami kerugian yang signifikan. Hal ini dikarenakan mekanisme penganggaran yang berlaku di PSIK sebagian besar berasal dari penganggaran yang dilakukan di awal. Setiap tahunnya PSIK akan menganggarkan beberapa peralatan yang digunakan untuk menunjang fungsi dan tugas mereka. Penganggaran ini dapat berupa penganggaran *hardware* seperti *hardisk* dan lain sebagainya. Kegiatan pencadangan ini bertujuan untuk mengantisipasi apabila sewaktu-waktu terjadi ancaman risiko, maka PSIK tidak perlu mengajukan anggaran dana kembali dan menunggu lebih lama untuk melakukan perbaikan. Selain itu sebagian besar biaya yang dikeluarkan oleh PSIK berasal dari pembaruan dan bukan berasal dari perbaikan.

Selanjutnya dilihat dari segi produktivitas, karyawan PSIK memiliki jam kerja dari jam 08.00 – 16.00 WIB. Untuk ancaman risiko ringan hingga sedang jam kerja karyawan PSIK tidak mengalami peningkatan. Hal tersebut dikarenakan apabila risiko-risiko tersebut dapat dikerjakan atau diselesaikan selama jam

kerja, maka akan langsung diselesaikan saat jam kerja sedang berlangsung. Namun, apabila risiko-risiko yang terjadi tergolong berat, maka karyawan akan mendapatkan jam kerja tambahan sebesar 50% - 75% dari jam kerja normal.

Kemudian dari segi kesehatan, karyawan PSIK belum pernah mendapatkan masalah kesehatan serius yang diakibatkan oleh ancaman risiko yang terjadi. Belum pernah terjadi masalah kesehatan pada karyawan hingga mengakibatkan diperlukannya perawatan rumah sakit. Beberapa karyawan hanya pernah mengalami sakit ringan akibat mengatasi risiko seperti kebocoran air pada ruang *server* dan mereka membutuhkan istirahat selama 1-2 hari. Sedangkan dari segi lainnya, PSIK belum pernah mengalami ancaman risiko yang kemudian menghasilkan permasalahan denda atau berurusan dengan regulasi hukum.

2. Identifikasi Aset Organisasi

OCTAVE-S mengidentifikasi aset organisasi ke dalam dua jenis aset, diantaranta aset informasi, sistem dan aplikasi (*information, systems dan application*); serta aset manusia (*people*). Berikut merupakan hasil identifikasi aset organisasi yang dilakukan pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya.

a. Aset Organisasi (Informasi, Sistem dan Aplikasi)

Tabel 4.6 Aset Organisasi (Informasi, Sistem dan Aplikasi)

No.	Aset Organisasi (Informasi, Sistem dan Aplikasi)	Keterangan
1.	FILKOM Apps	FILKOM Apps mengintegrasikan seluruh bagian yang ada pada Fakultas Ilmu Komputer melalui modul-modul yang ada di dalamnya seperti Sistem Keuangan, Sistem Kepegawaian, hingga Sistem Kemahasiswaan. FILKOM Apps berfungsi untuk mendukung jalannya proses bisnis yang ada di Fakultas Ilmu Komputer.
2.	Infrastruktur Data dan Jaringan	Infrastruktur data dan jaringan merupakan pendukung berjalannya seluruh sistem dan jaringan yang ada.
3.	Standar Operasional Prosedur (SOP)	Pedoman untuk menyelesaikan pekerjaan sesuai dengan fungsi dan tugas masing-masing.

Dalam menjalankan kegiatan operasionalnya, Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer mengembangkan sebuah sistem bernama FILKOM Apps yang digunakan sebagai sistem utama untuk mendukung aktivitas tugas dan fungsi organisasi. FILKOM Apps berfungsi

untuk membantu mengolah data dan informasi tentang kepegawaian hingga kemahasiswaan. Aset-aset lain yang memiliki keterkaitan dengan FILKOM Apps diantara lain Sistem Keuangan, Sistem Kepegawaian, Sistem Kemahasiswaan dan konten berita. Sistem-sistem tersebut merupakan modul-modul yang dikembangkan di dalam FILKOM Apps. Sedangkan layanan yang digunakan untuk mendukung tugas dan fungsi FILKOM Apps diantara lain *web server* dan layanan internet.

Aset kedua yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer adalah infrastruktur data dan jaringan yang digunakan untuk menunjang keseluruhan aktivitas yang ada pada organisasi. Aset-aset lain yang memiliki keterkaitan dengan infrastruktur data dan jaringan diantara lain *server*, jaringan internal, *workstation*, dan media penyimpanan yang digunakan untuk menyimpan data dan informasi yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Sedangkan layanan yang digunakan untuk mendukung tugas dan fungsi infrastruktur data dan jaringan diantara lain *database* dan koneksi internet.

Aset selanjutnya yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer adalah Standar Operasional Prosedur (SOP) yang digunakan sebagai pedoman untuk menyelesaikan pekerjaan sesuai dengan fungsi dan tugas masing-masing. Keberadaan SOP ini penting bagi Unit PSIK untuk memudahkan mereka dalam mengelola masuknya instruksi atau permintaan pembuatan layanan dan lain-lain yang berkaitan dengan aplikasi atau perbaikan terhadap sistem.

b. Aset Organisasi (Orang)

Tabel 4.7 Aset Organisasi (Orang)

No.	Aset Organisasi (Orang)	Keterangan
1.	Denny Sagita, S.Kom, M.Kom	Ketua Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer sebagai penanggung jawab utama dari seluruh aktivitas yang dikerjakan oleh PSIK.
2.	Thusti Dwi Purnami, A. Md	Koordinator Divisi Pengembangan Sistem Informasi yang bertanggung jawab untuk mengembangkan dan mengelola sistem informasi.
3.	Ivan Yulfrian, S.Kom	Koordinator Divisi Infrastruktur Data dan Jaringan yang bertanggung jawab untuk mengawasi dan mengelola seluruh infrastruktur data dan jaringan yang digunakan.

No.	Aset Organisasi (Orang)	Keterangan
4.	Edwin Ibnu Kautsar, S.Kom	Koordinator Divisi Multimedia dan Desain yang bertanggung jawab untuk mengelola bidang multimedia dan menyediakan suplai aset yang akan digunakan sebagai dasar untuk desain sistem informasi yang akan dikembangkan seperti gambar, *mockup*, dan lain sebagainya.

Selain aset organisasi berupa informasi, sistem dan aplikasi, Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer juga memiliki empat orang yang kemudian diidentifikasi sebagai aset organisasi dalam bentuk orang (*people*). Empat orang tersebut memiliki keahlian dan kemampuan yang penting dan sulit untuk digantikan. Keempat orang tersebut adalah Bapak Denny Sagita selaku Ketua Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer bertanggung jawab terhadap seluruh aktivitas unit, memimpin dan mengawasi kinerja dari seluruh karyawan Unit PSIK. Bapak Denny juga memiliki kemampuan untuk mentranslasikan permintaan yang ditujukan dari atasan atau peminta layanan kepada karyawan PSIK. Selain itu beliau juga membantu mencari atau mendapatkan data atau informasi yang dibutuhkan oleh tim.

Kemudian Ibu Thusti Dwi Purnami selaku Koordinator Divisi Pengembangan Sistem Informasi yang bertanggung jawab mengembangkan dan mengelola sistem informasi; Bapak Ivan Yulfrian selaku Koordinator Divisi Infrastruktur Data dan Jaringan yang bertanggung jawab untuk mengawasi dan mengelola seluruh infrastruktur data dan jaringan yang digunakan; dan Bapak Edwin Ibnu Kautsar selaku Koordinator Divisi Multimedia dan Desain yang bertanggung jawab untuk mengelola bidang multimedia dan menyediakan suplai aset yang akan digunakan sebagai dasar untuk desain sistem informasi yang akan dikembangkan seperti gambar, *mockup*, dan lain sebagainya.

3. Evaluasi Praktik Keamanan Organisasi

a. Kesadaran dan Pelatihan Keamanan

Tabel 4.8 Kesadaran dan Pelatihan Keamanan

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Anggota staf memahami peran dan tanggung jawab mereka terhadap keamanan masing-masing. Terdapat dokumentasi yang dapat diverifikasi.	√		

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
2.	Terdapat pencatatan pemantauan atau enkripsi yang berlaku untuk semua layanan, mekanisme, dan teknologi yang digunakan. Terdapat dokumentasi yang dapat diverifikasi.		√	
3.	Terdapat pelatihan dan pengingat tentang kesadaran keamanan untuk semua staff yang dilakukan secara periodik. Terdapat dokumentasi yang dapat diverifikasi kesesuaiannya secara berkala.			√
4.	Anggota staf mengikuti praktik keamanan yang baik, seperti • mengamankan informasi yang menjadi tanggung jawab mereka • tidak memberitahukan informasi sensitif kepada orang lain (penolakan terhadap rekayasa sosial) • memiliki kemampuan yang memadai untuk menggunakan perangkat keras dan perangkat lunak teknologi informasi • menggunakan praktik kata sandi yang baik • memahami dan mengikuti kebijakan dan peraturan keamanan • mengenali dan melaporkan apabila terjadi insiden	√		

PSIK telah memiliki kesadaran keamanan yang cukup baik. Para karyawan telah memahami peran dan tanggung jawab terhadap keamanan yang diterapkan didalam organisasi. Hal tersebut dapat dilihat dari *logbook tool-tool* yang digunakan untuk memantau kinerja sistem dan infrastruktur seperti jaringan dan lain sebagainya. Karyawan juga memiliki kemampuan yang memadai dalam menggunakan baik perangkat lunak dan perangkat keras teknologi informasi.

Selain itu karyawan PSIK juga telah mengikuti praktik keamanan yang baik seperti mengamankan informasi yang menjadi tanggung jawab masing-masing, menggunakan kata sandi untuk melindungi informasi yang mereka miliki, tidak memberitahukan informasi-informasi penting kepada orang-orang yang tidak memiliki hak akses, serta memahami dan mengikuti kebijakan dan peraturan yang berlaku untuk praktik keamanan. PSIK juga melakukan pencatatan terhadap pemantauan atau enkripsi yang dilakukan terhadap semua layanan dan teknologi yang digunakan namun tidak didokumentasikan. Selain itu karyawan PSIK menerima

pelatihan dari luar dan bukan dari organisasi. Pelatihan yang dilakukan didasari oleh inisiatif pribadi dari masing-masing karyawan.

b. Strategi Keamanan

Tabel 4.9 Strategi Keamanan

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Keamanan menjadi salah satu pertimbangan dalam strategi bisnis organisasi secara rutin.	√		
2.	Strategi dan kebijakan keamanan yang diterapkan juga mempertimbangkan strategi dan tujuan bisnis organisasi.	√		
3.	Strategi, tujuan, dan sasaran keamanan didokumentasikan, ditinjau, diperbarui, dan dikomunikasikan kepada organisasi secara rutin.			√

Fakultas Ilmu Komputer selalu mempertimbangkan masalah keamanan PSIK ketika menyusun strategi bisnis organisasi. Hal tersebut penting untuk melindungi data dan informasi yang mereka dimiliki. Strategi dan kebijakan keamanan juga menjadi salah satu pertimbangan dalam strategi dan tujuan bisnis yang dimiliki oleh PSIK. Namun belum terdapat dokumentasi yang jelas dan dapat diverifikasi untuk strategi, tujuan dan sasaran keamanan.

c. Manajemen Keamanan

Tabel 4.10 Manajemen Keamanan

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Manajemen mengalokasikan dana dan sumber daya yang cukup untuk kegiatan keamanan informasi.		√	
2.	Mendefinisikan peran dan tanggung jawab keamanan untuk semua staf dalam organisasi.	√		
3.	Semua staf melaksanakan peran dan tanggung jawab yang ditugaskan untuk keamanan informasi.	√		
4.	Ada prosedur terdokumentasi untuk memberi wewenang dan mengawasi semua staf (termasuk personel dari organisasi pihak ketiga) yang bekerja dengan informasi sensitif	√		

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
	atau yang bekerja di lokasi tempat informasi berada.			
5.	Organisasi memperhitungkan masalah keamanan informasi ketika merekrut dan memutuskan kontrak terhadap staff.			√
6.	Organisasi mengelola risiko keamanan informasi, termasuk • menilai risiko terhadap keamanan informasi • mengambil langkah-langkah untuk mengurangi risiko keamanan informasi	√		
7.	Manajemen menerima dan memberikan tindakan terhadap laporan rutin yang merangkum informasi terkait keamanan (misalnya, audit, log, risiko, dan penilaian kerentanan).			√

Dalam hal menjalankan manajemen keamanannya PSIK berkoordinasi langsung dengan UPT TIK Universitas Brawijaya sebagai pusat pengelolaan teknologi informasi di Universitas Brawijaya, sehingga sumber daya yang dialokasikan untuk kegiatan keamanan informasi akan dikelola langsung oleh UPT TIK Universitas Brawijaya. Seluruh karyawan PSIK juga telah melaksanakan peran dan tanggung jawab mereka dalam hal keamanan informasi.

Selain itu PSIK juga telah memiliki prosedur yang terdokumentasi untuk memberikan wewenang dan mengawasi seluruh karyawan yang dimiliki. PSIK juga telah melaksanakan proses pengelolaan risiko keamanan informasi seperti melakukan penilaian risiko keamanan informasi dan mengambil langkah-langkah untuk mengurangi risiko tersebut. Namun PSIK masih belum memperhitungkan masalah keamanan informasi ketika merekrut ataupun memutuskan kontrak terhadap karyawan yang mereka miliki. Hal ini dikarenakan proses rekruitmen yang dilakukan langsung oleh pihak Universitas Brawijaya tanpa menentukan kebutuhan terhadap jenis karyawan secara spesifik.

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

d. Peraturan dan Kebijakan Keamanan

Tabel 4.11 Peraturan dan Kebijakan Keamanan

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Organisasi memiliki serangkaian kebijakan yang terdokumentasi yang secara berkala ditinjau dan diperbarui.	√		
2.	Ada proses terdokumentasi untuk manajemen kebijakan keamanan, termasuk ketika melakukan • penciptaan dan pembuatan • administrasi (termasuk tinjauan dan pembaruan berkala) • komunikasi		√	
3.	Organisasi memiliki proses terdokumentasi untuk mengevaluasi dan memastikan kepatuhan terhadap kebijakan keamanan informasi, hukum dan peraturan yang berlaku, serta persyaratan asuransi.	√		
4.	Organisasi memberlakukan kebijakan keamanan yang seragam.	√		

Organisasi PSIK memiliki serangkaian kebijakan yang terdokumentasi yang secara berkala ditinjau dan diperbarui. PSIK memberlakukan kebijakan keamanan yang dibuat oleh UPT TIK Universitas Brawijaya dan diikuti oleh seluruh organisasi TIK dibawahnya. PSIK juga memiliki proses yang terdokumentasi untuk mengevaluasi dan memastikan kepatuhan organisasi terhadap kebijakan keamanan informasi, hukum dan peraturan yang berlaku.

e. Manajemen Keamanan Kolaboratif

Tabel 4.12 Manajemen Keamanan Kolaboratif

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Organisasi memiliki kebijakan dan prosedur untuk melindungi informasi ketika bekerja dengan organisasi eksternal (misalnya, pihak ketiga, kolaborator, subkontraktor, atau mitra), termasuk • melindungi informasi milik organisasi lain • memahami kebijakan keamanan dan prosedur organisasi eksternal • mengakhiri akses informasi dengan memberhentikan personil eksternal	√		
2.	Organisasi mendokumentasikan kebutuhan perlindungan informasi dan secara eksplisit mengkomunikasikannya kepada semua pihak ketiga yang sesuai.			√
3.	Organisasi memiliki mekanisme formal untuk memverifikasi bahwa semua organisasi pihak ketiga, layanan keamanan yang dialihdayakan, mekanisme, dan teknologi memenuhi *needs* dan *requirement*-nya.	√		
4.	Organisasi memiliki kebijakan dan prosedur untuk dapat bekerjasama dengan semua organisasi pihak ketiga yang • memberikan pelatihan kesadaran keamanan dan layanan • mengembangkan kebijakan keamanan untuk organisasi • mengembangkan rencana *contingency* untuk organisasi	√		

PSIK memiliki kebijakan dan prosedur untuk melindungi informasi ketika bekerja dengan organisasi eksternal yang bertujuan untuk melindungi data dan informasi baik yang dimiliki oleh PSIK maupun organisasi eksternal tersebut. Kebutuhan perlindungan informasi tidak melalui proses dokumentasi namun hanya dilakukan pembatasan akses informasi secara langsung kepada pihak eksternal. Namun PSIK juga memiliki prosedur atau mekanisme formal yang digunakan untuk memverifikasi bahwa semua organisasi pihak ketiga telah dapat

memenuhi *needs* dan *requirement*-nya.PSIK memiliki kebijakan dan prosedur untuk dapat bekerjasama dengan semua organisasi pihak ketiga. Hal tersebut dilakukan dengan melalui MoU apabila pihak ketiga tersebut berasal dari lingkup lokal dan melalui *International Office* apabila pihak ketiga tersebut berasal dari luar negeri.

f. Perencanaan *Contingency* atau Pemulihan Bencana (*Contingency Planning/Disaster Recovery*)

Tabel 4.13 Perencanaan Contingency atau Pemulihan Bencana

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Melakukan analisis terhadap operasi, aplikasi, dan kekritisan data.	√		
2.	Organisasi memiliki dokumentasi tentang • kelangsungan bisnis atau rencana operasi darurat • rencana pemulihan bencana • rencana darurat untuk menanggapi keadaan darurat yang dapat ditinjau dan diuji secara berkala.	√		
3.	*Contingency, disaster recovery,* dan *business continuity plans* mempertimbangkan kebutuhan dan kontrol terhadap akses fisik dan elektronik.	√		
4.	Semua staf • sadar akan *contingency, disaster recovery, dan business continuity plans* • memahami dan mampu menjalankan tanggung jawab mereka	√		

PSIK telah melakukan analisis terhadap operasi, aplikasi, dan kekritisan data. Organisasi memiliki dokumentasi tentang kelangsungan bisnis atau rencana operasi darurat, rencana pemulihan bencana, rencana darurat untuk menanggapi keadaan darurat yang dapat ditinjau dan diuji secara berkala. Selain itu *contingency planning, disaster recovery,* dan *business continuity* plans yang dimiliki juga mempertimbangkan kebutuhan dan kontrol terhadap akses baik fisik maupun elektronik. Kebutuhan terhadap rencana kelangsungan dan pemulihan setelah terjadinya bencana ini juga dipahami dengan baik oleh seluruh karyawan dan mereka mampu menjalankan tanggung jawab mereka dengan baik.

g. Pengendalian Akses Fisik

Tabel 4.14 Pengendalian Akses Fisik

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Terdapat dokumentasi rencana dan prosedur keamanan fasilitas yang teruji untuk menjaga tempat, bangunan, dan setiap area yang terlarang.		√	
2.	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengelola pengunjung aset fisik.		√	
3.	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengontrol akses fisik ke area kerja serta media perangkat keras (komputer, perangkat komunikasi, dll.) dan perangkat lunak.		√	
4.	Menjaga *workstation* dan komponen lain yang dapat digunakan untuk mengakses informasi sensitif secara fisik untuk mencegah akses yang tidak sah.	√		

Seluruh akses fisik dikelola langsung oleh pihak PSIK sendiri. Tidak terdapat dokumentasi rencana dan prosedur keamanan fasilitas yang teruji untuk menjaga tempat, bangunan, dan setiap area yang terlarang. Kebutuhan terhadap fasilitas hanya didasarkan pada referensi atau standar yang diberlakukan secara umum. PSIK tidak memiliki kebijakan dan prosedur yang terdokumentasi secara tertulis untuk mengelola pengunjung aset fisik, namun hanya orang-orang tertentu saja yang memiliki akses untuk mengunjungi aset fisik. Kontrol akses fisik pada media perangkat lunak maupun perangkat keras juga tidak didokumentasikan, namun kontrol tersebut dilakukan dengan menggunakan sistem yang telah terpasang pada *workstation* dan hanya orang-orang tertentu saja yang dapat mengakses informasi sensitif secara fisik pada *workstation* tersebut.

h. Pemantauan dan Audit Keamanan Fisik

Tabel 4.15 Pemantauan dan Audit Keamanan Fisik

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Catatan pemeliharaan (*maintenance*) disimpan untuk mendokumentasikan perbaikan dan modifikasi komponen fisik yang dilakukan terhadap fasilitas.	√		
2.	Tindakan individu atau kelompok, sehubungan dengan semua media yang dikontrol secara fisik, dapat dipertanggungjawabkan.	√		
3.	Memeriksa catatan audit dan pemantauan secara rutin untuk menganalisis adanya anomali (ketidaknormalan), serta mengambil tindakan korektif sesuai kebutuhan.		√	

Proses pemantauan dan audit keamanan fisik juga dilakukan sendiri oleh pihak internal PSIK. PSIK melakukan pencatatan pemeliharaan (*maintenance*) yang kemudian disimpan untuk mendokumentasikan setiap perbaikan dan modifikasi yang dilakukan terhadap komponen fisik. Setiap tindakan individu atau kelompok, yang berhubungan dengan semua media yang dikontrol secara fisik dapat dipertanggungjawabkan. PSIK juga melakukan audit dan pemantauan secara rutin untuk menganalisis adanya anomali (ketidaknormalan), serta mengambil tindakan korektif sesuai kebutuhan. Namun proses audit dan pemantauan tersebut tidak didokumentasikan secara tertulis.

i. Manajemen Jaringan dan Sistem

Tabel 4.16 Manajemen Jaringan dan Sistem

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Terdapat rencana keamanan yang terdokumentasi dan teruji untuk menjaga sistem dan jaringan.		√	
2.	Melindungi informasi sensitif dengan menggunakan penyimpanan yang aman (misalnya membuat cadangan yang disimpan di luar situs).	√		

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
3.	Memverifikasi integritas perangkat lunak yang terinstal secara teratur.	√		
4.	Semua sistem sudah diperbarui sesuai dengan revisi, *patch*, dan rekomendasi yang ada di dalam laporan keamanan.	√		
5.	Ada rencana yang terdokumentasi dan teruji untuk pencadangan perangkat lunak dan data. Semua staf memahami tanggung jawab mereka di bawah rencana tersebut.		√	
6.	Merencanakan, mengendalikan, dan mendokumentasikan perubahan yang dilakukan pada perangkat keras dan perangkat lunak TI.	√		
7.	Anggota staf TI mengikuti prosedur saat mengeluarkan (membuat), mengubah, dan mengakhiri kata sandi, akun, dan hak pengguna dari para pengguna. • Memerlukan identifikasi pengguna yang unik untuk semua pengguna sistem informasi, termasuk pengguna pihak ketiga. • Menghapus akun default dan kata sandi *default* dari sistem.		√	
8.	Hanya layanan yang diperlukan yang berjalan di sistem (menghapus semua layanan yang tidak perlu).	√		
9.	Menggunakan alat dan mekanisme untuk sistem keamanan dan administrasi jaringan, yang secara rutin ditinjau, diperbarui atau diganti.	√		

Manajemen jaringan dan sistem milik PSIK dikelola oleh internal organisasi. PSIK memiliki rencana keamanan yang terdokumentasi untuk menjaga sistem dan jaringan namun hasil dokumentasi tersebut belum teruji. PSIK juga menggunakan media penyimpanan yang aman untuk melindungi data dan informasi mereka. Selain menggunakan media penyimpanan secara fisik, PSIK juga memiliki media penyimpanan cadangan lain seperti dengan menggunakan *cloud.* Seluruh perangkat lunak yang terinstal akan selalu diverifikasi integritasnya secara teratur. PSIK melakukan perencanaan, pengendalian dan pendokumentasian

setiap perubahan yang dilakukan baik pada perangkat lunak maupun perangkat keras. Pembaruan pada sistem yang dilakukan menyesuaikan dengan revisi, patch, dan rekomendasi yang diberikan atau diinisiasi dari vendor. Setelah vendor melakukan pemberitahuan untuk melakukan revisi maka akan langsung diekseskusi oleh PSIK.

Organisasi PSIK memiliki rencana untuk melakukan pencadangan perangkat lunak dan data namun tidak didokumentasikan secara jelas. Selain itu proses mengeluarkan atau membuat, mengubah, dan mengakhiri baik kata sandi, akun dan hak akses pengguna menggunakan prosedur umum yang dikeluarkan oleh UPT TIK Universitas Brawijaya. Selain itu PSIK juga menggunakan alat dan mekanisme untuk memantau sistem keamanan dan administrasi jaringan yang akan ditinjau dan diperbarui secara rutin. Serta memberlakukan aturan dimana hanya layanan yang diperlukan yang akan berjalan di sistem.

j. Pemantauan dan Audit Keamanan TI

Tabel 4.17 Pemantauan dan Audit Keamanan TI

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Organisasi menggunakan alat untuk melakukan pemantauan (*monitoring*) dan audit (*auditing*) terhadap sistem dan jaringan secara rutin. Menangani aktivitas yang tidak biasa sesuai dengan kebijakan atau prosedur yang tepat.	√		
2.	Melakukan audit secara berkala pada *firewall* dan komponen keamanan lainnya untuk mematuhi kebijakan.	√		

PSIK menggunakan alat yang digunakan untuk melakukan pemantauan (*monitoring*) dan audit (*auditing*) terhadap sistem dan jaringan seperti melakukan pengecekan terhadap status *router* dan koneksi Wi-Fi. PSIK juga menggunakan *firewall* yang selalu mengalami proses audit untuk melindungi sistem dan jaringan mereka dari akses-akses tidak sah yang berasal dari luar organisasi.

k. Autentikasi dan Otorisasi

Tabel 4.18 Autentikasi dan Otorisasi

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Terdapat kontrol akses yang sesuai dan otentikasi pengguna (misalnya, izin file, konfigurasi jaringan) yang konsisten dengan kebijakan untuk membatasi akses pengguna ke informasi, sistem sensitif, aplikasi dan layanan tertentu, dan koneksi jaringan.	√		
2.	Ada kebijakan dan prosedur terdokumentasi untuk menetapkan dan menghentikan hak akses informasi bagi individu dan kelompok.	√		
3.	Menyediakan metode atau mekanisme untuk memastikan bahwa informasi sensitif belum diakses, diubah, atau dihancurkan dengan cara yang tidak sah. Metode atau mekanisme tersebut ditinjau dan diverifikasi secara berkala.			√

PSIK mengatur kontrol akses pengguna dengan menggunakan nas.ub.ac.id untuk membatasi akses pengguna ke dalam informasi, sistem, aplikasi atau layanan, serta akses ke dalam koneksi jaringan yang dimiliki. Proses penetapan dan penghentian hak akses pengguna diatur langsung oleh UPT TIK Universitas Brawijaya. Hal ini disebabkan karena keseluruhan data baik mahasiswa dan lain sebagainya berada langsung di pusat, sehingga apabila terjadi perubahan data pengguna yang ada di pusat maka secara otomatis pengguna tersebut juga tidak akan dapat mengakses layanan yang dimiliki oleh PSIK.

l. Manajemen Kerentanan

Tabel 4.19 Manajemen Kerentanan

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Terdapat satu prosedur terdokumentasi untuk mengelola kerentanan (*vulnerability*), termasuk • memilih alat evaluasi kerentanan, *checklist*, dan skrip • tetap *up to date* terhadap jenis kerentanan yang telah diketahui		√	

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
	beserta metode penyerangannya • meninjau sumber informasi tentang pernyataan kerentanan, peringatan keamanan, dan pemberitahuan • mengidentifikasi komponen infrastruktur untuk dievaluasi • menjadwalkan pelaksanaan evaluasi kerentanan • mengartikan dan menanggapi hasil • menjaga keamanan media penyimpanan dan menghilangkan kerentanan data/data yang rentan.			
2.	Mengikuti prosedur manajemen kerentanan (*vulnerability*) serta melakukan peninjauan dan perbaruan pada prosedur tersebut secara berkala.		√	
3.	Melakukan penilaian kerentanan teknologi secara berkala, kemudian menangani kerentanan yang teridentifikasi.	√		

Manajemen kerentanan juga dikelola langsung oleh internal organisasi. PSIK masih belum memiliki prosedur yang tertulis dengan jelas mengenai manajemen kerentanan organisasi. Prosedur manajemen kerentanan yang berlaku berasal dari UPT TIK Universitas Brawijaya yang kemudian diikuti oleh seluruh unit TIK fakultas di seluruh universitas. UPT TIK Universitas Brawijaya akan melakukan pelatihan mengenai manajemen kerentanan kepada seluruh unit TIK dibawahnya yang kemudian akan dilaksanakan pada fakultas masing-masing. Pelatihan tersebut akan membantu masing-masing unit TIK fakultas untuk melakukan penilaian kerentanan teknologi secara berkala, kemudian menangani kerentanan yang telah teridentifikasi.

m. Enkripsi

Tabel 4.20 Enkripsi

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Menggunakan kontrol keamanan yang sesuai ketika menyimpan informasi penting dan selama masa transmisi untuk melindungi informasi tersebut (misalnya, enkripsi data,	√		

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
	teknologi jaringan pribadi virtual).			
2.	Menggunakan protokol terenkripsi ketika mengelola sistem, *router*, dan *firewall* dari jarak jauh.	√		

PSIK menggunakan kontrol keamanan yang sesuai ketika menyimpan informasi penting untuk melindungi data dan informasi yang dimiliki. Selain itu PSIK juga menggunakan protokol yang terenkripsi ketika mengelola sistem, *router*, dan *firewall* dari jarak jauh.

n. Perancangan dan Arsitektur Keamanan

Tabel 4.21 Perancangan dan Arsitektur Keamanan

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Arsitektur sistem dan desain untuk sistem baru dan yang direvisi mempertimbangkan • strategi keamanan, kebijakan, dan prosedur • sejarah pemahaman terhadap keamanan • hasil penilaian risiko keamanan	√		
2.	Organisasi memiliki diagram terbaru yang menunjukkan arsitektur keamanan dan topologi jaringan *enterprise-wide* (mencakup seluruh aspek perusahaan).	√		

Arsitektur sistem dan desain untuk sistem baru dan sistem yang telah direvisi mempertimbangkan strategi keamanan, kebijakan, prosedur, serta hasil penilaian risiko keamanan. Penilaian risiko atau evaluasi yang dilakukan akan berasal dari masing-masing fakultas yang kemudia dilaporkan ke UPT TIK pusat. Kemudian setelah proses perbaikan selesai dilakukan maka akan dikembalikan kepada Unit TIK fakultas. Selain itu PSIK juga memiliki diagram terbaru yang menunjukkan arsitektur keamanan dan topologi jaringan yang digunakan.

o. Manajemen Insiden

Tabel 4.22 Manajemen Insiden

No.	Pernyataan	*Very Much*	*Some what*	*Not At All*
1.	Terdapat prosedur yang terdokumentasi untuk mengidentifikasi, melaporkan dan menanggapi adanya dugaan insiden keamanan dan pelanggaran yang terjadi.	√		
2.	Prosedur manajemen insiden diuji, diverifikasi, dan diperbarui secara berkala.			√
3.	Terdapat kebijakan dan prosedur yang terdokumentasi untuk bekerja dengan lembaga penegak hukum.			√

PSIK memiliki prosedur yang terdokumentasi untuk mengidentifikasi, melaporkan dan menanggapi adanya dugaan insiden keamanan dan pelanggaran yang terjadi. Namun PSIK masih belum memiliki prosedur manajemen insiden yang dapat diuji, diverifikasi, dan diperbarui secara berkala. Serta masih belum memiliki kebijakan dan prosedur yang terdokumentasi untuk bekerja dengan lembaga penegak hukum untuk mengatasi ancaman risiko yang terjadi.

4. Status *Stoplight* (*Stoplight Status*)

Setelah melakukan evaluasi praktik keamanan dengan menggunakan *Security Practices Worksheet* untuk mengetahui dan mendokumentasikan praktik yang diberlakukan oleh organisasi, kemudian dilakukan penilaian status *stoplight* untuk menentukan area praktik keamanan mana yang nantinya akan dimitigasi. Selain untuk mengetahui praktik keamanan yang telah dilaksanakan oleh organisasi, *Security Practices Worksheet* juga berfungsi untuk melihat seberapa efektif praktik tersebut dijalankan.

Tabel 4.23 Status *Stoplight*

No.	Aspek Keamanan	*Very Much*	*Some what*	*Not At All*	*Don't Know*	*Stoplight*
1.	Kesadaran dan Pelatihan Keamanan	2	1	1	0	Hijau
2.	Strategi Keamanan	2	0	1	0	Hijau
3.	Manajemen Keamanan	4	1	2	0	Hijau

No.	Aspek Keamanan	*Very Much*	*Some what*	*Not At All*	*Don't Know*	*Stoplight*
4.	Peraturan dan Kebijakan Keamanan	3	2	0	0	Hijau
5.	Manajemen Keamanan Kolaboratif	3	0	1	0	Hijau
6.	Perencanaan *Contingency*/Pemulihan Bencana	4	0	0	0	Hijau
7.	Pengendalian Akses Fisik	1	3	0	0	Kuning
8.	Pemantauan dan Audit Keamanan Fisik	2	1	0	0	Hijau
9.	Manajemen Jaringan dan Sistem	6	3	0	0	Hijau
10.	Pemantauan dan Audit Keamanan TI	2	0	0	0	Hijau
11.	Autentikasi dan Otorisasi	2	0	1	0	Kuning
12.	Manajemen Kerentanan	1	2	0	0	Kuning
13.	Enkripsi	2	0	0	0	Hijau
14.	Perancangan dan Arsitektur Keamanan	2	0	0	0	Hijau
15.	Manajemen Insiden	1	0	2	0	Merah

Dari hasil evaluasi dan penilaian yang dilakukan pada area praktik keamanan organisasi didapatkan status *stoplight* dari masing-masing area. Terdapat 11 area yang mendapatkan status lampu Hijau atau *Green Stoplight*, artinya organisasi telah menjalankan area praktik kemanan tersebut dengan sangat baik sehingga tidak membutuhkan perbaikan apapun. Kemudian 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 yang terakhir 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.

4.2.1.2 Proses 2 – Membuat Profil Ancaman

1. Memilih Aset Kritis

Terdapat beberapa aset kritis yang dimiliki oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer, diantara lain:

Tabel 4.24 Aset Kritis

No.	Aset Kritis	Keterangan
1.	FILKOM Apps	FILKOM Apps mengintegrasikan seluruh bagian yang ada pada Fakultas Ilmu Komputer melalui modul-modul yang ada di dalamnya seperti Sistem Keuangan, Sistem Kepegawaian, hingga Sistem Kemahasiswaan. FILKOM Apps berfungsi untuk mendukung jalannya proses bisnis yang ada di Fakultas Ilmu Komputer.
2.	Infrastruktur Data dan Jaringan	Infrastruktur data dan jaringan merupakan pendukung berjalannya seluruh sistem dan jaringan yang ada.

a. FILKOM Apps

FILKOM Apps merupakan salah satu inovasi yang diciptakan oleh Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. FILKOM Apps merupakan sebuah sistem informasi yang terintegrasi dengan proses bisnis yang berjalan pada Fakultas Ilmu Komputer. Hal tersebut bertujuan untuk mengurangi manualisasi yang dilakukan oleh civitas akademik, serta memudahkan dalam pengelolaan data dan informasi. FILKOM Apps berisi modul-modul sistem penting yang saling terintegrasi. Modul-modul tersebut berfungsi untuk mendukung jalannya proses bisnis yang ada di Fakultas Ilmu Komputer seperti Sistem Keuangan, Sistem Kepegawaian, hingga Sistem Kemahasiswaan. Seluruh data dan informasi yang berada di dalamnya saling berkesinambungan satu dengan lainnya. FILKOM Apps dapat diakses oleh semua pihak internal Fakultas Ilmu Komputer seperti dosen, karyawan dan mahasiswa.

FILKOM Apps mengintegrasikan seluruh bagian yang ada di Fakultas Ilmu Komputer seperti bagian akademik, kemahasiswaan, kepegawaian, keuangan, sekretariat, hingga laboratorium. Sistem yang dimiliki oleh FILKOM Apps membantu mengatur aktivitas yang dimiliki oleh bagian-bagian tersebut seperti pengelolaan jadwal kuliah, aktivitas belajar dan mengajar, kegiatan mahasiswa, hingga peminjaman fasilitas yang dimiliki oleh Fakultas Ilmu Komputer. Oleh karena itu, kehadiran FILKOM Apps dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik Fakultas Ilmu Komputer.

b. Infrastruktur Data dan Jaringan

Infrastruktur data dan jaringan dinilai menjadi aset kritis berikutnya yang harus dilindungi dari ancaman risiko yang mungkin terjadi pada PSIK.

Infrastruktur data dan jaringan merupakan pendukung berjalannya seluruh sistem dan jaringan yang ada. Selain itu infrastruktur data dan jaringan juga dinilai memiliki tingkat kerentanan yang cukup tinggi terhadap risiko. Hal tersebut dapat disebabkan oleh akses tidak sah yang berasal dari orang-Orang tidak bertanggung jawab dan lain sebagainya.

2. Mengidentifikasi Kebutuhan Keamanan untuk Aset Kritis

Tabel 4.25 Kebutuhan Keamanan untuk Aset Kritis

Aset Kritis	Kebutuhan Keamanan	Kebutuhan Keamanan yang Paling Dibutuhkan
FILKOM Apps	*Confidentiality* *Integrity* *Availability*	*Availability*
Infrastruktur Data dan Jaringan	*Confidentiality* *Integrity* *Availability*	*Integrity*

Berdasarkan hasil wawancara yang dilakukan dengan para karyawan Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer, didapati bahwa kerahasiaan informasi, integritas data, dan ketersediaan informasi menjadi kebutuhan keamanan untuk seluruh aset kritis yang dimiliki. Namun kebutuhan keamanan yang paling penting untuk FILKOM Apps adalah ketersediaan data dan informasi untuk para penggunanya. Karena data dan informasi yang terdapat pada FILKOM Apps harus selalu tersedia kapanpun pengguna layanan membutuhkan. Selain itu tanpa tersedianya data dan informasi tersebut maka proses bisnis yang ada pada Fakultas Ilmu Komputer tidak akan berjalan dengan baik. Kemudian kebutuhan keamanan yang paling penting untuk infrastruktur data dan jaringan adalah integritas. Hal tersebut karena infrastruktur data dan jaringan merupakan pendukung utama berjalannya seluruh sistem dan layanan yang ada pada Fakultas Ilmu Komputer. Selain itu, apabila infrastruktur data dan jaringan tidak utuh maka akan mengganggu fungsi dan tugas dari seluruh sistem dan layanan yang berjalan pada Fakultas Ilmu Komputer.

3. Mengidentifikasi Ancaman terhadap Aset Kritis

Pada langkah ini dilakukan idenifikasi terhadap jalur akses yang digunakan untuk dapat mengakses aset kritis, baik melalui jalur jaringan maupun jalur fisik. Sedangkan untuk identifikasi jenis aktor terbagi menjadi dua jenis, yaitu aktor yang dapat berasal dari dalam atau internal organisasi maupun yang berasal dari luar atau eksternal organisasi. Kemudian untuk motif yang digunakan ketika melakukan tindakan yang dapat menimbulkan ancaman risiko terbagi menjadi dua, yaitu dengan sengaja maupun tidak sengaja.

Selanjutnya kriteria untuk hasil yang didapatkan ketika ancaman risiko tersebut terjadi dibagi menjadi empat, diantaranya menghasilkan penyingkapan atau penyebaran informasi, modifikasi terhadap data dan informasi, perusakan atau penghancuran, serta interupsi. Dari tiga aset milik Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer, selanjutnya dipilih dua aset yang kemudian diidentifikasi menjadi aset kritis, antara lain FILKOM Apps, Infrastruktur Data dan Jaringan.

a. Pelaku Ancaman

Langkah ini menjelaskan mengenai pelaku atau aktor ancaman untuk setiap metode ancaman yang telah disebutkan berdasarkan motif pelaku dan jenis aktor. Berikut merupakan penjelasan untuk masing-masing aset kritis:

i. FILKOM Apps

Tabel 4.26 Pelaku Ancaman pada FILKOM Apps

Jalur Akses	Aktor	Motif	Bentuk Risiko
Jaringan	Internal	Tidak Sengaja	Pengguna FILKOM Apps melakukan kesalahan ketika menginputkan data.
		Sengaja	Dosen dan mahasiswa mata kuliah jaringan yang sedang melakukan uji coba jaringan atau mengerjakan tugas.
Fisik	Internal	Sengaja	Pemotongan kabel *mouse* komputer laboratorium.
	Eksternal	Tidak Sengaja	Teknisi yang memperbaiki sesuatu di atap namun mengakibatkan atap retak yang kemudian mengakibatkan kebocoran ketika hujan.
Masalah Sistem	Sistem Macet *(System Crashes*)		Layanan MySQL yang putus sehingga menyebabkan keseluruhan layanan yang didukung oleh MySQL tersebut menjadi *down*.
	Kerusakan *Hardware*		Pertama, *hardisk* yang digunakan penuh hingga sistem tidak dapat melakukan pembersihan tehadap *cache* sehingga menyebabkan pengguna layanan tidak dapat melakukan *login*. Kedua, *hardisk master* dan *slave* rusak.

Pada akses jaringan, ancaman risiko dari sisi internal yang dilakukan secara tidak sengaja dapat berasal dari semua pengguna FILKOM Apps yang salah memasukkan data sehingga dapat merusak

data yang telah tersimpan. Hal ini disebabkan oleh tidak adanya sosialisasi yang dilakukan oleh pihak PSIK terkait dengan modul baru yang dikembangkan. Selain itu juga terkadang dapat menimbulkan eror pada sistem. Namun hal tersebut dapat diatasi dengan menghapus data-data yang dianggap sampah serta melakukan perbaikan pada sistem sehingga lebih mudah digunakan oleh pengguna. Sedangkan ancaman risiko yang dilakukan secara sengaja dapat berasal dari mahasiswa atau dosen mata kuliah jaringan yang sedang menjalankan kegiatan belajar mengajar atau sedang megerjakan tugas. Hal tersebut seringkali terjadi namun masih dapat diatasi karena penggunakan *firewall* sehingga tidak mengganggu jalannya sistem.

Kemudian pada akses jaringan, ancaman risiko dari sisi eksternal yang dilakukan secara tidak sengaja belum pernah terjadi. Sedangkan ancaman risiko yang dilakukan secara sengaja dapat berasal dari pencurian data dan informasi yang dapat dilakukan oleh *hacker*. Namun hal ini juga tidak pernah terjadi karena penggunaan *firewall* yang selalu diperbarui pada PSIK.

Pada akses fisik, ancaman risiko dari sisi internal yang dilakukan secara tidak sengaja dapat berasal dari semua karyawan yang memiliki akses ke infratruktur pendukung sistem seperti *server* dan *workstation* kemudian secara tidak sengaja mengganggu kinerja alat-alat tersebut namun sejauh ini belum pernah terjadi. Sedangkan ancaman risiko yang dilakukan secara sengaja dapat berasal dari orang-orang yang bertindak kriminal dengan tujuan untuk merusak fasilitas pendukung FILKOM Apps. Seperti yang pernah terjadi adalah seseorang dengan sengaja memotong kabel *mouse* komputer bersama pada laboratorium.

Pada akses fisik, ancaman risiko dari sisi internal yang dilakukan secara tidak sengaja dapat berasal dari kesalahan pengguna ketika mengoperasikan FILKOM Apps sehingga akan menimbulkan eror. Sedangkan ancaman risiko yang dilakukan secara sengaja dapat berasal dari orang-orang yang menginstall aplikasi lain seperti aplikasi *game* sehingga menyebabkan gangguan pada sistem FILKOM Apps yang sedang berjalan. Selain itu juga dapat berasal dari pengguna yang bertindak kriminal dengan tujuan untuk merusak fasilitas pendukung FILKOM Apps. Seperti yang pernah terjadi adalah seseorang dengan sengaja memotong kabel *mouse* komputer bersama pada laboratorium.

Kemudian pada akses fisik, ancaman risiko dari sisi eksternal yang dilakukan secara tidak sengaja dapat berasal dari teknisi PLN yang sedang menjalankan tugasnya namun tidak sengaja mengganggu aliran listrik yang digunakan. Kemudian seperti yang pernah terjadi yaitu seorang teknisi yang memperbaiki sesuatu di atap namun mengakibatkan atap retak. Sehingga ketika terjadi hujan atap tersebut

bocor. Selain itu ancaman dapat berasal dari siswa magang yang tidak sengaja merusak fasilitas fisik pendukung sistem ketika sedang bekerja. Sedangkan ancaman risiko yang dilakukan secara sengaja dapat berasal dari pihak-pihak diluar organisasi yang ingin merusak atau mencuri infratrukstur penunjang FILKOM Apps seperti *server* dan *workstation*.

Selanjutnya risiko yang muncul dan berasal dari masalah sistem sendiri yang pernah dialami oleh FILKOM Apps diantaranya *system crashes* atau sistem macet. Hal ini disebabkan oleh layanan MySQL yang putus sehingga menyebabkan keseluruhan layanan yang didukung oleh MySQL tersebut menjadi *down*. Namun hal tersebut dapat dengan segera diatasi oleh pihak PSIK sehingga tidak menimbulkan kerugian lebih lanjut. Sedangkan data yang tersimpan masih tetap dapat terlindungi dan tersedia ketika dibutuhkan.

Risiko berikutnya berasal dari *hardware* yang digunakan mengalami kecacatan atau kerusakan. *Hardisk* yang digunakan untuk menyimpan data dan informasi oleh FILKOM Apps penuh hingga sistem tidak dapat melakukan pembersihan tehadap *cache*. Hal tersebut berdampak pada pengguna layanan tidak dapat melakukan *login* atau masuk ke dalam aplikasi. Selanjutnya risiko yang muncul akibat *hardisk master* dan *slave* yang rusak. Namun hal tersebut juga langsung dapat diatasi dengan mengganti *hardisk* yang rusak tersebut dengan *hardisk* lain yang telah dicadangkan di awal.

Sedangkan untuk risiko yang berasal dari *software defect* atau kecacatan sistem dan *malicious code* atau kode berbahaya belum pernah terjadi pada aplikasi FILKOM Apps. Hal tersebut dikarenakan seluruh sistem yang digunakan oleh PSIK telah dilindungi oleh *firewall* yang terinstall. Sehingga dapat meminimalisir kemungkinan ancaman yang berasal dari luar dengan melalui jaringan.

ii. Infrastruktur Data dan Jaringan

Tabel 4.27 Pelaku Ancaman pada Infrastruktur Data dan Jaringan

Jalur Akses	Aktor	Motif	Bentuk Risiko
Jaringan	Internal	Tidak Sengaja	Penumpukan paket di *router* yang berasal dari komputer karyawan maupun dosen.
		Sengaja	Dosen dan mahasiswa mata kuliah jaringan yang sedang melakukan uji coba jaringan atau mengerjakan tugas.
	Eksternal	Sengaja	Adanya *brute force attack*.
Fisik	Eksternal	Tidak Sengaja	Teknisi yang memperbaiki sesuatu di atap namun mengakibatkan atap retak yang kemudian mengakibatkan kebocoran ketika hujan.

Jalur Akses	Aktor	Motif	Bentuk Risiko
Masalah Lainnya	Masalah *Power supply*		Penggunaan trafo dengan *voltage* yang tidak sesuai dengan standar.
	Bencana Alam		Petir dan hujan deras yang mengakibatkan kebocoran.

Pada akses jaringan, dari sisi internal pernah terjadi ancaman risiko berupa menumpuknya paket di *router* yang tidak sengaja dilakukan baik oleh karyawan maupun dosen. Paket-paket tersebut berasal dari komputer yang mereka gunakan. Hal ini menyebabkan klien atau pengguna tersebut sementara harus diblokir atau dihentikan aksesnya hingga pengguna tersebut menyadari bahwa akses yang dimiliki tidak dapat digunakan. Selanjutnya akan dilakukan perbaikan oleh pihak PSIK dan mengembalikan akses pengguna tersebut. Kemudian dari sisi internal, sering terjadi ancaman risiko yang dilakukan dengan sengaja berasal dari mahasiswa yang sedang mengerjakan tugas yang berhubungan dengan jaringan. Serangan yang dilakukan masih dalam tahap yang mampu dikenali dan dapat diatasi dengan segera. Selain itu juga pernah terjadi serangan-serangan lain namun tidak pernah berhasil sepenuhnya dan dapat dengan cepat diatasi, sehingga tidak sampai menimbulkan dampak yang signifikan.

Sedangkan pada sisi eksternal, sering terjadi serangan yang berasal dari luar organisasi dan dilakukan dengan sengaja. Serangan tersebut sebagian besar berasal dari *brute force attack* dan dianggap sebagai serangan yang paling umum terjadi. Namun masih dapat diatasi dengan menggunakan *firewall* yang dipasang oleh PSIK, dampak yang paling signifikan dirasakan oleh pengguna adalah jaringan yang terasa lebih lambat dari biasanya.

Pada akses fisik, sering terjadi ancaman risiko yang berasal dari ketidaksengajaan yang dilakukan oleh pihak internal PSIK seperti tidak sengaja melakukan tindakan yang berpotensi mengganggu atau merusak infrastruktur yang terpasang. Hal tersebut dapat terjadi karena kondisi infrastruktur yang dimiliki dan terpasang di ruangan PSIK sangat *compromise* atau membahayakan seperti peralatan yang berserakan dan tidak terkoordinasi dengan baik namun sejauh ini belum pernah terjadi. Selain itu tidak ada sistem proteksi yang baik dan benar atau sesuai dengan standar. Dampak yang dihasilkan dari ancaman risiko jenis ini adalah terjadinya interupsi hingga jaringan yang *down*. Kemudian ancaman risiko dari sisi eksternal yang dilakukan secara tidak sengaja yang pernah terjadi berasal dari seorang teknisi yang memperbaiki sesuatu di atap namun mengakibatkan atap retak. Sehingga ketika terjadi hujan atap tersebut bocor.

Selanjutnya terdapat masalah lain yang pernah terjadi pada infrastruktur PSIK seperti masalah *power supply* serta bencana alam.

Masalah *power supply* yang terjadi diakibatkan oleh trafo dengan *voltage* yang tidak sesuai dengan standar, terlalu rendah dan frekuensi yang dimiliki kurang dari 60 Hz. Dampak yang dihasilkan dari risiko jenis ini adalah rusaknya beberapa komputer karena aliran listrik yang tidak stabil.

Kemudian masalah akibat bencana alam yang pernah terjadi berupa petir dan hujan. Petir yang terjadi pada tahun 2014 memberikan dampak yang cukup signifikan bagi organisasi diantaranya tiga buah *router* rusak dan *access point* mati sehingga mengakibatkan koneksi internet di beberapa tempat mengalami masalah. Selain itu juga menghasilkan kerugian dari segi keuangan yang cukup besar bagi organisasi berupa perbaikan-perbaikan yang menghabiskan sekitar Rp 300.000.000,00. Berikutnya hujan deras yang mengakibatkan sejumlah air masuk ke dalam ruang *server*. Dampak yang dihasilkan dari bencana hujan ini tidak begitu signifikan dan dapat diatasi dengan segera oleh karyawan PSIK.

b. Tingkat Motif dan Keyakinan

i. FILKOM Apps

Tabel 4.28 Tingkat Keyakinan Motif pada FILKOM Apps

Jalur Akses	Aktor	Motif	Tingkat Motif
Jaringan	Internal	Tidak Sengaja	Rendah
		Sengaja	Rendah - Sedang
Fisik	Internal	Sengaja	Sedang
	Eksternal	Tidak Sengaja	Rendah - Sedang
Masalah Sistem	Sistem Macet *(System Crashes*)		Rendah
	Kerusakan *Hardware*		Rendah

Melalui akses jaringan, tingkat motif yang dimiliki oleh pihak internal yang dilakukan dengan tidak sengaja adalah rendah. Hal ini dikarenakan dampak yang dihasilkan tidak terlalu signifikan dan masih dapat diatasi oleh pihak PSIK dengan penghapusan data-data yang dinilai tidak benar atau sampah. Sedangkan tingkat motif yang dimiliki oleh pihak internal yang dilakukan dengan sengaja adalah rendah hingga sedang. Selanjutnya melalui akses jaringan, tingkat motif yang dimiliki oleh pihak eksternal yang dilakukan dengan sengaja adalah sedang hingga tinggi. Hal ini dikarenakan sejauh ini belum ada serangan yang menghasilkan dampak signifikan yang dihasilkan oleh ancaman-ancaman risiko tersebut. Serangan-serangan yang dilakukan masih dapat ditangani oleh karyawan PSIK. Hal ini karena penggunaan *antivirus* dan *firewall* yang dipasang serta diperbarui secara berkala.

Melalui akses fisik, tingkat motif yang dimiliki oleh pihak internal yang dilakukan dengan secara tidak sengaja adalah rendah karena

masih sangat jarang terjadi. Sedangkan tingkat motif yang dimiliki oleh pihak internal yang dilakukan dengan sengaja adalah sedang. Selanjutnya melalui akses fisik, tingkat motif yang dimiliki oleh pihak eksternal yang dilakukan secara tidak sengaja adalah rendah hingga sedang karena masih jarang terjadi. Sedangkan tingkat motif yang dimiliki oleh pihak eksternal yang dilakukan dengan sengaja adalah sedang.

Selanjutnya melalui permasalahan yang muncul pada sistem. Tingkat motif atau keyakinan terjadinya sistem yang macet atau tidak dapat dioperasikan (*system crashes*) adalah rendah karena pihak PSIK selalu melakukan pengecekan dan *maintenance* yang dilakukan secara berkala. Selain itu juga melakukan pembaruan terhadap *software-software* yang digunakan untuk menghindari kemungkinan sistem yang macet karena ketidak sesuaian versi. Kemudian tingkat motif atau keyakinan terjadinya kerusakan terhadap *hardware* (*hardware defect*) adalah rendah. Hal ini dikarenakan PSIK selalu menyediakan atau mengalokasikan *hardware* cadangan untuk infrastruktur penunjang sistem mereka.

ii. Infrastruktur Data dan Jaringan

Tabel 4.29 Tingkat Keyakinan Motif pada Infrastruktur Data dan Jaringan

Jalur Akses	Aktor	Motif	Tingkat Keyakinan Motif
Jaringan	Internal	Tidak Sengaja	Rendah
		Sengaja	Rendah - Sedang
	Eksternal	Sengaja	Sedang - Tinggi
Fisik	Eksternal	Tidak Sengaja	Rendah - Sedang
Masalah Lainnya	Masalah *Power supply*		Rendah
	Bencana Alam		Tinggi

Melalui akses jaringan, motif yang dimiliki oleh pihak internal yang dilakukan dengan tidak sengaja adalah rendah. Sedangkan melalui akses jaringan, motif yang dimiliki oleh aktor internal yang dilakukan dengan sengaja adalah rendah hingga sedang, karena tidak menghasilkan dampak yang signifikan dan masih dapat diatasi dengan penggunaan *firewall.* Kemudian melalui akses jaringan, motif yang dimiliki oleh pihak eksternal yang dilakukan dengan sengaja tergolong sedang hingga tinggi. Hal ini karena serangan yang terjadi sebagian besar berasal dari *brute force attack* atau serangan yang bertujuan untuk meretas kata sandi untuk dapat masuk ke dalam sistem.

Selanjutnya melalui akses fisik, motif yang dimiliki oleh pihak internal yang dilakukan dengan tidak sengaja adalah rendah. Hal ini dikarenakan kondisi infrastruktur yang dimiliki dan terpasang di ruangan PSIK sangat *compromise* atau membahayakan seperti

peralatan yang berserakan dan tidak terkoordinasi dengan baik. Sedangkan tingkat motif yang dimiliki oleh pihak eksternal yang dilakukan secara tidak sengaja adalah rendah hingga sedang karena masih jarang terjadi.

Selanjutnya melalui permasalahan yang muncul akibat faktor-faktor lain. Tingkat motif atau keyakinan terjadinya masalah terhadap *power supply* adalah rendah karena masih terdapat *power supply* yang belum memenuhi standar atau memenuhi kriteria kebutuhan perangkat keras untuk digunakan. Namun kerusakan yang diakibatkan masih dapat diatasi dengan menggunakan peralatan yang telah dicadangkan atau disiapkan setiap tahunnya. Kemudian Kemudian tingkat motif atau keyakinan terjadinya masalah akibat bencana alam adalah tinggi.

c. Data Frekuensi Kejadian Ancaman di Masa Lalu

i. FILKOM Apps

Tabel 4.30 Frekuensi Kejadian pada FILKOM Apps

Jalur Akses	Aktor	Motif	Frekuensi Kejadian
Jaringan	Internal	Tidak Sengaja	7 kali dalam 1 tahun pada tahun 2017.
		Sengaja	3 kali dalam 1 minggu.
Fisik	Internal	Sengaja	1 kali dalam 1 tahun.
	Eksternal	Tidak Sengaja	1 kali dalam 1 tahun.
Masalah Sistem	Sistem Macet *(System Crashes*)		2 kali dalam 1 tahun pada tahun 2017.
	Kerusakan *Hardware*		*Hardisk* penuh terjadi 1 kali dalam 1 tahun pada tahun 2016. *Hardisk* rusak terjadi 1 kali dalam 1 tahun pada tahun 2017.

Ancaman risiko yang terjadi melalui akses jaringan yang ditimbulkan oleh pihak internal yang dilakukan secara tidak sengaja seperti salah dalam memasukkan data pernah terjadi sebanyak tujuh kali dalam satu tahun kemarin. Sedangkan yang dilakukan secara sengaja seringkali terjadi namun tidak menghasilkan dampak yang signifikan sehingga masih dapat ditangani. Kemudian ancaman risiko yang terjadi melalui akses jaringan yang ditimbulkan oleh pihak eksternal yang dilakukan baik secara tidak sengaja maupun sengaja belum pernah terjadi karena adanya *antivirus* dan *firewall* yang dipasang oleh pihak PSIK.

Kemudian ancaman risiko yang terjadi melalui akses fisik yang ditimbulkan oleh pihak internal yang dilakukan secara tidak sengaja seperti kesalahan pengoperasian dan fasilitas yang rusak akibat kelalaian karyawan belum pernah terjadi. Sedangkan yang dilakukan secara sengaja seperti yang diakibatkan oleh perusakan fasilitas pendukung seperti pemotongan kabel *mouse* pernah terjadi sebanyak satu kali. Kemudian ancaman risiko yang terjadi melalui akses fisik yang ditimbulkan oleh pihak eksternal yang dilakukan secara tidak sengaja seperti atap bocor pernah terjadi sebanyak satu kali. Sedangkan yang dilakukan secara sengaja belum pernah terjadi.

Kemudian ancaman risiko yang berasal dari sistem yang macet atau tidak dapat dioperasikan (*system crashes)* pernah terjadi dua kali dalam satu bulan pada tahun 2017. Sedangkan *hardware defect* atau kecacatan dan kerusakan *hardware* diantaranya, *hardware* penuh pernah terjadi satu kali pada tahun 2016 dan dua buah *hardisk* rusak pernah terjadi satu kali pada tahun 2017.

ii. Infrastruktur Data dan Jaringan

Tabel 4.31 Frekuensi Kejadian pada Infrastruktur Data dan Jaringan

Jalur Akses	Aktor	Motif	Frekuensi Kejadian
Jaringan	Internal	Tidak Sengaja	3 kali dalam 1 minggu.
		Sengaja	3 kali dalam 1 minggu.
	Eksternal	Sengaja	Setiap hari
Fisik	Eksternal	Tidak Sengaja	1 kali dalam 1 tahun.
Masalah Lainnya	Masalah *Power supply*		1 kali dalam 1 tahun.
	Bencana Alam		Petir dan hujan deras masing-masing pernah terjadi 1 kali dalam 1 tahun.

Ancaman risiko yang terjadi melalui akses jaringan akibat pihak internal yang melakukan baik dengan sengaja maupun tidak sangat sering terjadi. Namun dampak yang dihasilkan tidak terlalu signifikan dan masih dapat ditangani. Sedangkan ancaman risiko yang terjadi melalui akses jaringan akibat pihak eksternal yang melakukan dengan sengaja terjadi beberapa kali. Dampak yang dihasilkanpun tidak besar karena PSIK telah menggunakan *firewall* untuk melindungi jaringan yang dimiliki. Kemudian ancaman risiko yang terjadi melalui akses fisik akibat pihak internal yang melakukan dengan sengaja jarang terjadi. Dampak yang dihasilkan berupa jaringan yang melambat.

Kemudian ancaman risiko yang terjadi melalui akses fisik yang ditimbulkan oleh pihak eksternal yang dilakukan secara tidak sengaja seperti atap bocor pernah terjadi sebanyak satu kali.

Sedangkan ancaman risiko yang terjadi akibat *power supply* yang bermasalah pernah terjadi beberapa kali dan menghasilkan dampak rusaknya beberapa komputer. Berikutnya risiko yang dihasilkan oleh bencana alam berupa petir pernah terjadi satu kali pada tahun 2014 dan hujan deras yang menyebabkan kebocoran ruang kerja pernah terjadi satu kali.

d. Identifikasi Potensi Ancaman

Langkah ini menyajikan contoh-contoh konkrit dari ancaman berdasarkan jenis aktor yang dibagi lagi berdasarkan motif pelaku ancaman, untuk setiap jenis akses dan aset kritis yang sering dibahas. Berikut penjelasannya untuk setiap aset kritis:

i. FILKOM Apps

Tabel 4.32 Potensi Ancaman pada FILKOM Apps

Jalur Akses	Aktor	Motif	Potensi Ancaman
Jaringan	Internal	Tidak Sengaja	Pengguna aplikasi lupa *logout* setelah selesai menggunakan komputer bersama, sehingga pengguna berikutnya dapat masuk ke dalam sistem dengan menggunakan ID yang sama.
		Sengaja	Pengguna menggunakan ID pengguna lainnya dan digunakan untuk mengubah atau menghapus data pemilik ID tersebut.
	Eksternal	Tidak Sengaja	Siswa magang yang diberikan kewenangan atau tugas untuk mengelola sistem namun tanpa sengaja mengganggu fungsi kerja sistem.
		Sengaja	Pihak luar organisasi yang melakukan serangan terhadap sistem dan jaringan yang dimiliki oleh PSIK.
Fisik	Internal	Tidak Sengaja	Karyawan yang tidak sengaja melakukan tindakan yang berpotensi mengganggu atau merusak infrastruktur yang terpasang.
		Sengaja	Karyawan organisasi yang sedang melakukan pemeliharaan (*maintenance*) secara berkala.
	Eksternal	Tidak Sengaja	Kontaktor yang sedang melakukan pembangunan gedung atau

Jalur Akses	Aktor	Motif	Potensi Ancaman
			penggalian tanah dan tidak sengaja merusak jaringan kabel yang terpasang.
		Sengaja	Orang luar yang ingin mengambil beberapa infrastruktur tanpa ijin dari organisasi.
Masalah Sistem	Kerusakan *Software*		Kurangnya pemeliharaan (*maintenance*) yang dilakukan oleh pihak internal organisasi.
	Sistem Macet *(System Crashes*)		
	Kerusakan *Hardware*		
	Kode-kode Berbahaya (virus, worm, trojan, dll)		

Potensi ancaman risiko melalui akses jaringan yang dilakukan oleh pihak internal secara tidak sengaja dapat berasal dari pengguna aplikasi yang lupa untuk keluar (*logout*) dari sistem setelah selesai menggunakan komputer bersama, sehingga pengguna berikutnya dapat masuk ke dalam sistem dengan menggunakan ID yang sama. Potensi ancaman risiko melalui akses jaringan yang dilakukan oleh pihak internal secara sengaja dapat berasal dari para pengguna yang dengan sengaja menggunakan ID pengguna lainnya dan digunakan untuk mengubah atau menghapus data pemilik ID tersebut. Potensi ancaman risiko melalui akses jaringan yang dilakukan oleh pihak eksternal secara tidak sengaja dapat berasal dari siswa magang yang diberikan kewenangan atau tugas untuk mengelola sistem namun tanpa sengaja mengganggu fungsi kerja sistem itu sendiri. Kemudian potensi ancaman risiko melalui akses jaringan yang dilakukan oleh pihak eksternal secara sengaja dapat berasal dari pihak luar organisasi yang melakukan serangan terhadap sistem dan jaringan yang dimiliki oleh PSIK. Hal ini berpotensi untuk merusak bahkan menghilangan data dan informasi yang dimiliki.

Potensi ancaman risiko melalui akses fisik yang dilakukan oleh pihak internal secara tidak sengaja dapat berasal dari para karyawan yang masuk ke ruang PSIK dan tanpa sengaja memberikan gangguan terhadap infrastruktur penunjang FILKOM Apps yang terpasang seperti *server* dan *workstation*. Hal ini disebabkan oleh kondisi infrastruktur yang dimiliki dan terpasang di ruangan PSIK sangat *compromise* atau membahayakan seperti peralatan yang berserakan dan tidak terkoordinasi dengan baik. Potensi ancaman risiko melalui akses fisik yang dilakukan oleh pihak internal secara sengaja dapat berasal dari para karyawan organisasi yang sedang melakukan pemeliharaan (*maintenance*) secara berkala sehingga akan menyebabkan sistem tidak dapat digunakan sementara waktu. Selain itu dapat berasal dari

karyawan yang melakukan perusakan atau pencurian terhadap infrastruktur penunjang sistem.

Potensi ancaman risiko melalui akses fisik yang dilakukan oleh pihak eksternal secara tidak sengaja dapat berasal dari orang-orang yang sedang melakukan pembangunan gedung atau penggalian tanah dan tidak sengaja merusak jaringan kabel yang terpasang. Selain itu juga dapat berasal dari petugas PLN yang melakukan kesalahan ketika melaksanakan pekerjaannya sehingga menyebabkan gangguan pada aliran listik. Potensi ancaman risiko melalui akses fisik yang dilakukan oleh pihak eksternal secara sengaja dapat berasal dari orang luar yang ingin mengambil beberapa infrastruktur tanpa ijin dari organisasi.

Kemudian potensi ancaman risiko yang berasal dari masalah terhadap sistem seperti *software* yang rusak atau cacat, *system crashes, hardware* yang rusak atau cacat, serta kode-kode berbahaya dapat berasal dari kurangnya tindakan pemeliharaan (*maintenance*) yang dilakukan oleh pihak internal organisasi. Selain itu tidak adanya antivirus atau firewall yang terpasang dapat berpotesi untuk membahayakan jaringan internal organisasi.

ii. Infrastruktur Data dan Jaringan

Tabel 4.33 Potensi Ancaman pada Infrastruktur Data dan Jaringan

Jalur Akses	Aktor	Motif	Potensi Ancaman
Jaringan	Internal	Tidak Sengaja	Kelalaian karyawan ketika mereka melakukan *maintenance* dan pembaruan terhadap *server*.
		Sengaja	Karyawan organisasi yang sedang melakukan pemeliharaan (*maintenance*) secara berkala.
	Eksternal	Tidak Sengaja	Kesalahan yang dilakukan oleh pihak ketiga yang menjadi rekan kerja atau *stakeholder* dari organisasi.
		Sengaja	Pencurian data dan informasi yang dilakukan oleh *hacker.*
Fisik	Internal	Tidak Sengaja	Pengguna melakukan *input* data dengan menggunakan komputer milik pengguna lain sehingga dapat mengakibatkan kerusakan data yang terdapat pada *database server.*
		Sengaja	Karyawan yang melakukan perusakan maupun pencurian infrastruktur.
	Eksternal	Tidak Sengaja	Petugas PLN yang melakukan kesalahan ketika melaksanakan pekerjaannya sehingga menyebabkan gangguan pada aliran listik.

Jalur Akses	Aktor	Motif	Potensi Ancaman
		Sengaja	Orang luar yang melakukan pecurian terhadap infrastruktur organisasi.
Masalah Lainnya	Masalah *Power supply*		Kurangnya evaluasi yang dilakukan oleh organisasi terhadap infrastruktur pendukung yang digunakan.
	Bencana Alam		Kurangnya kesiapan organisasi dalam mengantisipasi kejadian tersebut di masa yang akan datang.

Potensi ancaman risiko melalui akses jaringan yang dilakukan oleh pihak internal secara tidak sengaja dapat berasal dari kelalaian karyawan ketika mereka melakukan *maintenance* dan pembaruan terhadap *server*. Sedangkan yang dilakukan oleh pihak internal secara sengaja dapat berasal dari karyawan yang melakukan tindakan kriminal dengan cara mencuri data dan informasi organisasi untuk tujuan kejahatan. Selain itu juga dapat berasal dari kegiatan *maintenance* terhadap infrastruktur data dan jaringan yang dilakukan secara berkala sehingga akan menghentikan fungsi kerjanya sementara waktu. Kemudian potensi ancaman risiko yang dilakukan oleh pihak eksternal secara tidak sengaja dapat berasal dari kesalahan yang dilakukan oleh pihak ketiga yang menjadi rekan kerja atau *stakeholder* dari organisasi. Sedangkan yang dilakukan oleh pihak eksternal secara sengaja dapat berasal dari pencurian data dan informasi yang dilakukan oleh *hacker*.

Potensi ancaman risiko melalui akses fisik yang dilakukan oleh pihak internal secara tidak sengaja dapat berasal dari pengguna yang melakukan *input* data dengan menggunakan komputer milik pengguna lain sehingga dapat mengakibatkan kerusakan data yang terdapat pada *database server.* Sedangkan yang dilakukan oleh pihak internal secara sengaja dapat berasal dari karyawan yang melakukan tindakan kriminal seperti perusakan maupun pencurian infrastruktur yang dimiliki oleh organisasi. Kemudian potensi ancaman risiko melalui akses fisik yang dilakukan oleh pihak eksternal secara tidak sengaja dapat berasal dari orang-orang yang sedang melakukan pembangunan gedung atau penggalian tanah dan tidak sengaja merusak jaringan kabel yang terpasang. Selain itu juga dapat berasal dari petugas PLN yang melakukan kesalahan ketika melaksanakan pekerjaannya sehingga menyebabkan gangguan pada aliran listik. Sedangkan potensi ancaman risiko yang dilakukan oleh pihak eksternal secara sengaja dapat berasal dari orang-orang di luar organisasi yang melakukan pecurian terhadap infrastruktur organisasi.

Kemudian potensi ancaman risiko yang berasal dari masalah lain seperti *power supply* dapat berasal dari kurangnya evaluasi yang dilakukan oleh organisasi terhadap infrastruktur pendukung yang

digunakan. Sehingga *power supply* yang digunakan tidak lagi mampu menunjang spesifikasi yang dimiliki oleh perangkat-perangkat utama seperti komputer dan lain sebagainya. Sedangkan untuk ancaman risiko yang berasal dari bencana alam dapat disebabkan oleh kurangnya kesiapan organisasi dalam mengantisipasi kejadian tersebut di masa yang akan datang.

4.2.2 Fase 2: Mengidentifikasi Kerentanan Infrastruktur.

4.2.2.1 Proses 3 - Memeriksa Infrastruktur Komputer yang Berhubungan dengan Aset Kritis

Berdasarkan hasil wawancara yang dilakukan pada karyawan Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer, maka didapatkan hasil pengolahan data sebagai berikut:

1. Memeriksa Jalur Akses

Sistem yang memiliki keterkaitan paling erat dengan aset kritis yang ada pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer adalah FILKOM Apps. Sebagai sistem yang memiliki keterkaitan paling erat, FILKOM Apps memiliki beberapa kelas komponen yang berfungsi untuk mendukung tugas dan fungsinya, diantara lain *Servers, Internal Networks, On-Site Workstations,* Laptop, *Wireless Components* dan *Storage Devices.*

FILKOM Apps menggunakan komponen-komponen tersebut untuk mengirimkan informasi dan aplikasi kepada para pengguna layanan. *Servers* digunakan untuk menjalankan layanan yang disediakan oleh PSIK. *Internal* dan *External Networks* digunakan untuk mengakses informasi dan layanan. Hingga *Storage Devices* yang digunakan sebagai media penyimpanan data dan informasi yang dimiliki oleh PSIK.

2. Menganalisa Proses yang Terkait dengan Teknologi

Tabel 4.34 Kelas Komponen

No.	Komponen	Keterangan/Fungsi	Jumlah	Penanggung Jawab
1.	*Servers*	*Database*	1	Ivan Yulfrian
		File	1	
		Web server	1	
2.	*Internal Networks*	*Tunnel*	1	Ivan Yulfrian
3.	*On-Site Workstations*	Jaringan	1	Ivan Yulfrian
		Aplikasi	2	Thusti Dwi Purnami dan Dwi Saputro Nugroho
		Web Service	1	Thusti Dwi Purnami
4.	Laptop	Jaringan	1	Ivan Yulfrian
		Aplikasi	1	

No.	Komponen	Keterangan/Fungsi	Jumlah	Penanggung Jawab
5.	*Wireless Components*	Laptop		Pemilik dari perangkat masing-masing
		Handphone		
		Dan perangkat lainnya miliki karyawan, dosen dan mahasiswa		
6.	*Storage Devices.*	DS 3500 (fisik)	1	Ivan Yulfrian
		Cloud (non fisik)	1	

PSIK memiliki sekitar sepuluh *server* yang digunakan untuk menunjang tugas dan fungsinya dalam menyediakan layanan bagi pengguna. Untuk menjalankan FILKOM Apps sendiri terdapat tiga *server* utama yang digunakan, diantara lain untuk *database*, *file* dan *web service*. Orang yang bertanggung jawab untuk menjaga dan mengelola *server* ini adalah divisi infrastruktur data dan jaringan. PSIK sangat mempertimbangkan keamanan ketika mengkonfigurasi dan memelihara *server*. Data tersebut diperoleh dari hasil wawancara yang dilakukan pada staf divisi infrastruktur data dan jaringan. Jaringan internal yang digunakan oleh PSIK untuk mengelola layanan yang dimiliki adalah *tunnel*. Orang yang bertanggung jawab untuk menjaga dan mengelola jaringan internal ini adalah divisi infrastruktur data dan jaringan. Keamanan juga menjadi suatu pertimbangan yang pasti ketika mengkonfigurasi dan memelihara jaringan internal.

Kemudian PSIK juga memiliki kurang lebih empat *On-Site Workstations* yang digunakan untuk mendukung fungsi dan tugasnya, diantaranya satu buah *workstation* yang digunakan untuk mengelola jaringan dan dibawahi langsung oleh divisi infrastruktur data dan jaringan; dua buah *workstation* yang digunakan untuk mengelola aplikasi FILKOM Apps dan dibawahi langsung oleh divisi pengembangan sistem informasi; serta satu buah *workstation* yang digunakan untuk mengelola *web service* dan dibawahi langsung oleh divisi pengembangan sistem informasi.

Selanjutnya terdapat dua buah laptop yang digunakan oleh PSIK ketika sedang melakukan survey atau kegiatan yang berada diluar ruangan. Laptop-laptop tersebut masing-masing digunakan untuk mengelola jaringan dan aplikasi. Keduanya berada dibawah tanggung jawab divisi infrastruktur data dan jaringan. Berikutnya terdapat beberapa jenis *wireless components* yang dapat digunakan oleh penguna untuk mengakses layanan yang disediakan oleh PSIK diantaranya laptop, handphone, dan peralatan lain baik milik mahasiswa, dosen atau karyawan Fakultas Ilmu Komputer. Keamanan semua perangkat tersebut menjadi tanggung jawab dari masing-masing pemilik. Dan kelas komponen yang terakhir adalah *Storage Device*. Terdapat dua jenis media penyimpanan yang digunakan oleh PSIK untuk menyimpan data dan informasi yang dimiliki, yaitu berbentuk fisik dan non-fisik. Untuk media penyimpanan berbentuk fisik, PSIK menggunakan *storage* seri DS 3500 sebanyak dua buah. Kemudian untuk media penyimpanan berbentuk non-fisik, PSIK menggunakan *cloud.* Media

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

penyimpanan ini menjadi tanggung jawab dari divisi infrastruktur data dan jaringan.

4.2.3 Fase 3: Mengembangkan Strategi Perlindungan dan Rencana Keamanan.

4.2.3.1 Proses 4 - Identifikasi dan Analisis Risiko

Berdasarkan hasil wawancara yang dilakukan pada karyawan Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer, maka didapatkan hasil pengolahan data sebagai berikut:

1. Mengevaluasi Dampak Ancaman

Terdapat beberapa jenis dampak yang dapat diterima oleh organisasi apabila terjadi ancaman risiko, diantara lain penyingkapan atau penyebaran data dan informasi (*disclosure*), modifikasi data dan informasi (*modification*), kerusakan atau penghancuran (*loss, destruction*), serta interupsi (*interuption*). Dampak-dampak tersebut kemudian akan dapat mempengaruhi reputasi, keuangan, produktivitas, denda, hingga kesehatan.

Tabel 4.35 Evaluasi Dampak Ancaman

No.	Kriteria	Jenis Dampak	Nilai
1.	Reputasi	Penyingkapan atau penyebaran (*Disclosure*)	Sedang
		Modifikasi (*Modification*)	Sedang
		Kerusakan atau penghancuran (*Loss, Destruction*)	Sedang
		Interupsi (*Interuption*)	Sedang
2.	Keuangan	Penyingkapan atau penyebaran (*Disclosure*)	Sedang
		Modifikasi (*Modification*)	Sedang
		Kerusakan atau penghancuran (*Loss, Destruction*)	Sedang
		Interupsi (*Interuption*)	Sedang
3.	Produktivitas	Penyingkapan atau penyebaran (*Disclosure*)	Rendah
		Modifikasi (*Modification*)	Rendah
		Kerusakan atau penghancuran (*Loss, Destruction*)	Rendah
		Interupsi (*Interuption*)	Rendah
4.	Denda	Penyingkapan atau penyebaran (*Disclosure*)	Rendah
		Modifikasi (*Modification*)	Rendah
		Kerusakan atau penghancuran (*Loss, Destruction*)	Rendah

No.	Kriteria	Jenis Dampak	Nilai
		Interupsi (*Interuption*)	Rendah
5.	Kesehatan	Penyingkapan atau penyebaran (*Disclosure*)	Rendah
		Modifikasi (*Modification*)	Rendah
		Kerusakan atau penghancuran (*Loss, Destruction*)	Rendah
		Interupsi (*Interuption*)	Rendah

a. Reputasi

Dampak yang dihasilkan oleh ancaman risiko pada reputasi bernilai sedang (*medium*) untuk semua jenis ancaman karena reputasi organisasi yang baik. Selain itu PSIK juga tidak pernah mengalami pengurangan atau kehilangan pelanggan yang diakibatkan oleh risiko yang terjadi. Hal tersebut dikarenakan sejauh ini belum ada sistem yang dapat digunakan sebagai alternatif untuk menggantikan tugas dan fungsi dari sistem yang dibuat oleh PSIK.

b. Keuangan

Dampak yang dihasilkan oleh ancaman risiko pada keuangan bernilai sedang (*medium*) untuk semua jenis ancaman. Hal ini dikarenakan peningkatan biaya operasional yang dialami oleh organisasi tidak melebihi dari 15% setiap tahunnya, serta organisasi tidak kehilangan pendapatan lebih dari 20% per tahunnya.

c. Produktivitas

Dampak yang dihasilkan oleh ancaman risiko pada produktivitas bernilai rendah (*low*) untuk semua jenis ancaman. Peningkatan jam kerja karyawan yang harus dialami tidak melebihi dari 10%. Hal ini dikarenakan sejauh ini ancaman risiko yang terjadi masih mampu untuk diatasi di waktu jam kerja dan tidak membutuhkan tambahan lainnya.

d. Denda

Dampak yang dihasilkan oleh ancaman risiko pada denda bernilai rendah (*low*) untuk semua jenis ancaman. Sejauh ini organisasi belum pernah mengalami ancaman risiko yang menghasilkan denda.

e. Kesehatan

Dampak yang dihasilkan oleh ancaman risiko pada kesehatan bernilai rendah (*low*) untuk semua jenis ancaman. Permasalahan kesehatan yang dialami oleh karyawan masih dapat diatasi dengan baik sehingga tidak sampai pada tahap kehilangan pada kehidupan.

2. Menetapkan Kriteria Evaluasi Probabilitas

Tabel 4.36 Evaluasi Probabilitas

Jalur Akses	Frekuensi Probabilitas	Keterangan
Jaringan	Tinggi	Masih sering terjadi serangan dengan frekuensi tiga kali dalam seminggu.

Jalur Akses	Frekuensi Probabilitas	Keterangan
Fisik	Rendah	Kondisi infrastruktur yang dimiliki dan terpasang di ruangan PSIK masih belum terkoordinasi dengan baik.
Masalah Sistem	Rendah	Risiko yang terjadi tidak melebihi dua kali dalam setahun.
Masalah Lainnya	Rendah	Risiko yang terjadi tidak melebihi dua kali dalam setahun.

Frekuensi terjadinya ancaman risiko pada organisasi yang melalui akses jaringan tergolong tinggi. Hal ini disebabkan karena masih sering terjadi serangan dari dalam internal maupun eksternal organisasi, baik yang disengaja maupun tidak. Menurut wawancara yang telah dilakukan dengan pihak PSIK, serangan tersebut paling sedikit terjadi tiga kali dalam seminggu. Rentang waktu tersebut masih tergolong dalam kriteria tinggi. Namun serangan-serangan yang muncul tersebut masih dapat ditanggulangi dengan baik karena PSIK telah menggunakan *firewall* untuk melindungi jaringan yang mereka gunakan.

Sedangkan frekuensi terjadinya ancaman risiko pada organisasi yang melalui akses fisik tergolong rendah. Hal ini disebabkan karena kondisi infrastruktur yang dimiliki dan terpasang di ruangan PSIK sangat *compromise* atau membahayakan seperti peralatan yang berserakan dan tidak terkoordinasi dengan baik. Sehingga masih terdapat kemungkinan orang-orang dapat mengganggu infrastruktur fisik secara tidak sengaja oleh pihak internal organisasi. Selanjutnya frekuensi terjadinya ancaman risiko pada organisasi yang berasal dari masalah terhadap sistem seperti *system crashes* dan kerusakan terhadap *hardware* masih tergolong rendah. Hal tersebut karena risiko yang terjadi tidak melebihi dua kali dalam setahun. Selain itu, risiko yang muncul masih dapat diatasi oleh pihak organisasi sehingga tidak sampai menghasilkan dampak yang signifikan.

Dan untuk frekuensi terjadinya ancaman risiko pada organisasi yang berasal dari masalah lainnya seperti masalah pada *power supply* dan bencana alam masih tergolong rendah. Hal ini karena ancaman-ancaman yang berasal dari kriteria ini terjadi kurang dari dua kali dalam satu tahun. Selain itu organisasi juga dapat menanggulangi risiko-risiko tersebut dengan baik sehingga tidak menimbulkan dampak lebih lanjut yang dapat membahayakan bagi organisasi.

3. Mengevaluasi Probabilitas Ancaman

Tabel 4.37 Probabilitas Ancaman

Jalur Akses	Aktor	Motif	Jenis Dampak	Nilai	Tingkat Keyakinan
Jaringan	Internal	Tidak Sengaja	Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Sedang

Jalur Akses	Aktor	Motif	Jenis Dampak	Nilai	Tingkat Keyakinan
			Modifikasi (*Modification*)	Rendah	Sedang
			Kerusakan atau penghancuran (*Loss, Destruction*)	Rendah	Rendah
			Interupsi (*Interuption*)	Sedang	Sedang
		Sengaja	Penyingkapan atau penyebaran (*Disclosure*)	Sedang	Besar
			Modifikasi (*Modification*)	Sedang	Besar
			Kerusakan atau penghancuran (*Loss, Destruction*)	Rendah	Rendah
			Interupsi (*Interuption*)	Sedang	Sedang
	Eksternal	Tidak Sengaja	Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Rendah
			Modifikasi (*Modification*)	Rendah	Rendah
			Kerusakan atau penghancuran (*Loss, Destruction*)	Rendah	Rendah
			Interupsi (*Interuption*)	Sedang	Sedang
		Sengaja	Penyingkapan atau penyebaran (*Disclosure*)	Sedang	Besar
			Modifikasi (*Modification*)	Sedang	Besar
			Kerusakan atau penghancuran (*Loss, Destruction*)	Rendah	Rendah
			Interupsi (*Interuption*)	Sedang	Sedang
Fisik	Internal	Tidak Sengaja	Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Rendah
			Modifikasi (*Modification*)	Rendah	Rendah
			Kerusakan atau	Sedang	Sedang

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Jalur Akses	Aktor	Motif	Jenis Dampak	Nilai	Tingkat Keyakinan
			penghancuran (*Loss, Destruction*)		
			Interupsi (*Interuption*)	Sedang	Sedang
		Sengaja	Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Rendah
			Modifikasi (*Modification*)	Rendah	Rendah
			Kerusakan atau penghancuran (*Loss, Destruction*)	Rendah	Rendah
			Interupsi (*Interuption*)	Rendah	Rendah
	Eksternal	Tidak Sengaja	Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Rendah
			Modifikasi (*Modification*)	Rendah	Rendah
			Kerusakan atau penghancuran (*Loss, Destruction*)	Sedang	Sedang
			Interupsi (*Interuption*)	Sedang	Sedang
		Sengaja	Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Rendah
			Modifikasi (*Modification*)	Rendah	Rendah
			Kerusakan atau penghancuran (*Loss, Destruction*)	Sedang	Sedang
			Interupsi (*Interuption*)	Sedang	Sedang
Masalah Sistem	Kerusakan *Software*		Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Rendah
			Modifikasi (*Modification*)	Rendah	Sedang
			Kerusakan atau penghancuran (*Loss, Destruction*)	Rendah	Sedang
			Interupsi	Rendah	Sedang

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Jalur Akses	Aktor	Motif	Jenis Dampak	Nilai	Tingkat Keyakinan
			(*Interuption*)		
	System Crashes		Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Rendah
			Modifikasi (*Modification*)	Sedang	Sedang
			Kerusakan atau penghancuran (*Loss, Destruction*)	Sedang	Sedang
			Interupsi (*Interuption*)	Sedang	Sedang
	Kerusakan *Hardware*		Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Rendah
			Modifikasi (*Modification*)	Sedang	Sedang
			Kerusakan atau penghancuran (*Loss, Destruction*)	Sedang	Sedang
			Interupsi (*Interuption*)	Sedang	Sedang
	Kode-kode Berbahaya		Penyingkapan atau penyebaran (*Disclosure*)	Sedang	Tinggi
			Modifikasi (*Modification*)	Sedang	Tinggi
			Kerusakan atau penghancuran (*Loss, Destruction*)	Sedang	Sedang
			Interupsi (*Interuption*)	Sedang	Sedang
Masalah Lainnya	Masalah *Power supply*		Penyingkapan atau penyebaran (*Disclosure*)	Rendah	Rendah
			Modifikasi (*Modification*)	Rendah	Rendah
			Kerusakan atau penghancuran (*Loss, Destruction*)	Sedang	Sedang
			Interupsi (*Interuption*)	Sedang	Sedang
	Bencana Alam		Penyingkapan atau penyebaran	Rendah	Rendah

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Jalur Akses	Aktor	Motif	Jenis Dampak	Nilai	Tingkat Keyakinan
			(*Disclosure*)		
			Modifikasi (*Modification*)	Rendah	Rendah
			Kerusakan atau penghancuran (*Loss, Destruction*)	Sedang	Sedang
			Interupsi (*Interuption*)	Sedang	Sedang

a. Peluang terjadinya ancaman yang secara tidak di sengaja disebabkan oleh pihak dalam perusahaan melalui akses jaringan.

Ancaman risiko yang berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi dan modifikasi terhadap data dan informasi bernilai rendah dengan tingkat keyakinan sedang dilihat dari kemungkinan yang ada di masa yang akan datang. Kemudian yang berpeluang untuk menghasilkan dampak perusakan atau penghilangan terhadap data dan informasi yang ada bernilai rendah dengan tingkat keyakinan rendah. Sedangkan risiko yang berpeluang untuk menghasilkan dampak interupsi bernilai sedang dengan tingkat keyakinan sedang dilihat dari seberapa besar potensi risiko tersebut akan mengganggu kinerja yang dimiliki oleh PSIK.

b. Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak dalam perusahaan melalui akses jaringan.

Ancaman risiko yang berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi dan modifikasi terhadap data dan informasi bernilai sedang dengan tingkat keyakinan besar dilihat dari seberapa kuat motif aktor ketika melakukan tindakan di masa yang akan datang. Kemudian yang berpeluang untuk menghasilkan dampak perusakan atau penghilangan terhadap data dan informasi yang ada bernilai rendah dengan tingkat keyakinan rendah. Sedangkan risiko yang berpeluang untuk menghasilkan dampak interupsi bernilai sedang dengan tingkat keyakinan sedang dilihat dari seberapa besar potensi risiko tersebut akan mengganggu kinerja yang dimiliki oleh PSIK.

c. Peluang terjadinya ancaman yang secara tidak di sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan.

Ancaman risiko yang berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran, modifikasi, serta perusakan atau penghilangan terhadap data dan informasi bernilai rendah dengan tingkat keyakinan rendah. Sedangkan risiko yang berpeluang untuk menghasilkan dampak interupsi bernilai sedang dengan tingkat keyakinan sedang dilihat

dari seberapa besar potensi risiko tersebut akan mengganggu kinerja yang dimiliki oleh PSIK.

d. Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan.

Ancaman risiko yang berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi dan modifikasi terhadap data dan informasi bernilai sedang dengan tingkat keyakinan besar dilihat dari seberapa kuat motif aktor ketika melakukan tindakan di masa yang akan datang. Kemudian yang berpeluang untuk menghasilkan dampak perusakan atau penghilangan terhadap data dan informasi yang ada bernilai rendah dengan tingkat keyakinan rendah. Sedangkan risiko yang berpeluang untuk menghasilkan dampak interupsi bernilai sedang dengan tingkat keyakinan sedang dilihat dari seberapa besar potensi risiko tersebut akan mengganggu kinerja yang dimiliki oleh PSIK.

e. Peluang terjadinya ancaman yang secara tidak di sengaja disebabkan oleh pihak dalam perusahaan melalui akses fisik.

Ancaman risiko yang berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi dan modifikasi terhadap data dan informasi bernilai rendah dengan tingkat keyakinan rendah. Sedangkan untuk ancaman risiko yang berpeluang untuk menghasilkan dampak perusakan atau penghilangan terhadap data dan informasi serta interupsi bernilai sedang dengan tingkat keyakinan sedang dilihat dari seberapa kuat motif aktor ketika melakukan tindakan di masa yang akan datang.

f. Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak dalam perusahaan melalui akses fisik.

Seluruh ancaman risiko yang bepeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi, modifikasi terhadap data dan informasi, perusakan atau penghilangan data dan informasi, serta interupsi bernilai rendah dengan tingkat keyakinan rendah.

g. Peluang terjadinya ancaman yang secara tidak di sengaja disebabkan oleh pihak luar perusahaan melalui akses fisik.

Ancaman risiko yang berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi dan modifikasi terhadap data dan informasi bernilai rendah dengan tingkat keyakinan rendah. Sedangkan untuk ancaman risiko yang berpeluang untuk menghasilkan dampak perusakan atau penghilangan terhadap data dan informasi serta interupsi bernilai sedang dengan tingkat keyakinan sedang dilihat dari seberapa kuat motif aktor ketika melakukan tindakan di masa yang akan datang.

h. Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak luar perusahaan melalui akses fisik.

Ancaman risiko yang berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi dan modifikasi terhadap data dan informasi bernilai rendah dengan tingkat keyakinan rendah. Sedangkan untuk ancaman risiko yang berpeluang untuk menghasilkan dampak perusakan atau penghilangan terhadap data dan informasi serta interupsi bernilai sedang dengan tingkat keyakinan sedang dilihat dari seberapa kuat motif aktor ketika melakukan tindakan di masa yang akan datang.

i. Peluang terjadinya ancaman melalui masalah pada sistem.

Ancaman risiko yang berasal dari kerusakan *software* dan berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi bernilai rendah dengan tingkat keyakinan rendah. Sedangkan yang berpeluang untuk menghasilkan dampak modifikasi terhadap data dan informasi, perusakan atau penghilangan data dan informasi, serta interupsi bernilai rendah dengan tingkat keyakinan sedang.

Kemudian ancaman risiko yang berasal dari *system crashes* dan berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi bernilai rendah dengan tingkat keyakinan rendah. Sedangkan yang berpeluang untuk menghasilkan dampak modifikasi terhadap data dan informasi, perusakan atau penghilangan data dan informasi, serta interupsi bernilai sedang dengan tingkat keyakinan sedang.

Selanjutnya ancaman risiko yang berasal dari kerusakan *hardware* dan berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi bernilai rendah dengan tingkat keyakinan rendah. Sedangkan yang berpeluang untuk menghasilkan dampak modifikasi terhadap data dan informasi, perusakan atau penghilangan data dan informasi, serta interupsi bernilai sedang dengan tingkat keyakinan sedang.

Dan ancaman risiko yang berasal dari kode-kode berbahaya seperti virus dan berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi serta modifikasi terhadap data dan informasi bernilai sedang dengan tingkat keyakinan tinggi. Sedangkan yang berpeluang untuk menghasilkan dampak perusakan atau penghilangan data dan informasi serta interupsi bernilai sedang dengan tingkat keyakinan sedang.

j. Peluang terjadinya ancaman melalui masalah lain.

Ancaman risiko yang berasal dari masalah terhadap *power supply* dan berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi serta modifikasi terhadap data dan informasi bernilai rendah dengan tingkat keyakinan rendah. Sedangkan yang

berpeluang untuk menghasilkan dampak perusakan atau penghilangan data dan informasi serta interupsi bernilai sedang dengan tingkat keyakinan sedang.

Kemudian ancaman risiko yang berasal dari bencana alam dan berpeluang untuk menghasilkan dampak penyingkapan atau penyebaran informasi serta modifikasi terhadap data dan informasi bernilai rendah dengan tingkat keyakinan rendah. Sedangkan yang berpeluang untuk menghasilkan dampak perusakan atau penghilangan data dan informasi serta interupsi bernilai sedang dengan tingkat keyakinan sedang.

4.2.3.2 *Failure Mode and Effect Analysis* (FMEA)

1. Identifikasi Potensi Mode Kegagalan (*Failure Mode*)

Potensi mode kegagalan yang digunakan dalam FMEA mengacu kepada kerentanan sistem informasi dan infrastruktur yang ada di dalam organisasi maupun perusahaan terhadap aspek-aspek yang sering terjadi sehingga menyebabkan kegagalan pada sistem dan mengganggu jalannya proses bisnis yang dimiliki. Seperti hasil identifikasi yang telah didapatkan dengan menggunakan kerangka kerja OCTAVE-S sebelumnya, berikut adalah mode kegagalan yang terdapat pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer:

a. Data pada *database* tidak valid, ketika pengguna dari sistem salah dalam memasukkan atau meng-*input* data.
b. Jaringan mengalami gangguan atau melambat, ketika terdapat gangguan yang berasal dari internal organisasi seperti praktik mata kuliah jaringan.
c. *Workstation* jaringan mengalami gangguan, ketika ada *brute force attack*.
d. *Mouse* komputer laboratorium rusak, ketika kabel penghubungnya dipotong.
e. Jaringan mengalami gangguan, ketika terjadi penumpukan paket di *router*.
f. Layanan yang didukung oleh MySQL mengalami penurunan, ketika layanan MySQL terputus.
g. *Hardisk* penuh, ketika *hardisk* tidak dapat menerima dan menyimpan data pengguna.
h. *Hardisk master* dan *slave* rusak, ketika *hardisk* tersebut tidak dapat digunakan.
i. Beberapa komputer mengalami kerusakan, ketika terjadi masalah pada *power supply* yaitu *voltage trafo* yang tidak sesuai dengan standar.
j. Ruang kerja mengalami kebanjiran, ketika terjadi hujan deras.
k. Pekerjaan staf terganggu hingga terhenti, ketika terjadi kebocoran akibat atap retak.
l. Jaringan internet melambat atau mengalami masalah, ketika beberapa *router* dan *access point* mati akibat petir.

2. Identifikasi Dampak Kegagalan Potensial

Potensi kegagalan yang muncul pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer menimbulkan beberapa dampak yang menghambat kinerja atau proses bisnis yang dimiliki. Data pada *database* yang tidak valid yang sering terjadi akan menyebabkan ketidaksesuaian antara data asli pengguna dengan data yang tersimpan pada *database*. Hal ini akan menghambat proses yang berhubungan dengan proses akademik pengguna.

Kemudian jaringan yang terganggu baik akibat gangguan internal, *brute force attack*, masalah pada *router* dan kerusakan *access point* yang diakibatkan oleh kesengajaan maupun bencana alam seperti petir dapat mengganggu dan menghambat jalannya proses bisnis yang mengharuskan adanya penggunaan jaringan. Akibatnya baik staf, dosen maupun mahasiswa yang menggunakan jaringan sebagai pendukung tidak dapat menjalankan tugas dan fungsi mereka sebagaimana mestinya. Terputusnya *mouse* komputer pada laboratorium akan mengakibatkan terhambatnya proses belajar mengajar karena komputer yang tidak dapat dioperasikan tanpa adanya *mouse* tersebut. Hal ini juga akan menyebabkan kerugian pada pihak organisasi.

Selanjutnya kerusakan *hardisk* maupun *hardisk* yang penuh akan menghambat kinerja server karena tidak dapat menerima dan menyimpan data. Selain itu kinerja sistem juga akan melambat karena *memory* yang ada telah penuh ataupun tidak ada lagi media penyimpanan yang dapat digunakan. Akibatnya proses bisnis yang seharusnya berjalan tidak dapat berfungsi dengan baik dan benar. Masalah berikutnya adalah komputer *workstation* yang rusak akibat *power supply* yang tidak sesuai standar. Hal ini berdampak pada terhambatnya kinerja staff Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer karena tidak dapat berkerja sebagaimana mestinya.

Permasalahan lain yang pernah muncul adalah bocornya atap ruang kerja Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer yang diakibatkan oleh seorang teknisi yang melakukan kesalahan ketika melakukan perbaikan di atap. Hal ini mengakibatkan ruang kerja mengalami kebanjiran ketika hujan deras tiba. Akibat lain yang ditimbulkan adalah terganggu hingga terhentinya aktivitas yang dilakukan oleh staf Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer. Hal ini tentu menghambat proses bisnis yang dimiliki oleh organisasi itu sendiri. Hasil identifikasi dari potensi mode kegagalan ini kemudian akan digunakan untuk melakukan penilaian terhadap tingkat keparahan dampak (*severity*) berdasarkan tingkat kepentingannya.

3. Menentukan Tingkat Keparahan Dampak (*Severity*)

Di bawah ini merupakan hasil penilaian tingkat keparahan dampak (*severity*) berdasarkan hasil analisis dari setiap potensi mode kegagalan yang ada pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer. Penilaian tersebut didasarkan pada kriteria penilaian yang dimiliki oleh tingkat keparahan dampak (*severity*) dan didapatkan hasil sebagai berikut:

Tabel 4.38 Tingkat Keparahan Dampak (*Severity*)

No.	Potensi Kegalalan	Tingkat Keparahan
1.	Data pada *database* tidak valid	7
2.	Jaringan terganggu karena gangguan dari internal	5
3.	*Workstation* jaringan mengalami gangguan akibat *brute force attack*	2
4.	*Mouse* rusak	4
5.	Jaringan terganggu karena penumpukan paket di *router*	5
6.	Layanan MySQL terputus	5
7.	*Hardisk* penuh	5
8.	*Hardisk master* dan *slave* rusak	6
9.	Komputer rusak karena *power supply*	6
10.	Ruang kerja bocor dan kebanjiran	5
11.	Jaringan internet melambat karena *router* dan *access point* mati akibat petir	6

Dari penilaian diatas didapatkan hasil bahwa sebagian besar risiko yang telah teridentifikasi pada Unit Pengelolaan Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer memiliki nilai tingkat keparahan dampak sebesar 5 dan 6. Nilai 5 pada kriteria keparahan dampak berarti bahwa risiko tersebut menghasilkan dampak yang moderat atau menyebabkan penurunan terhadap kinerja serta menimbulkan keluhan dari para penggunanya, sedangkan nilai 6 berarti bahwa risiko tersebut menghasilkan dampak yang signifikan atau menghasilkan kerugian berupa kerusakan parsial atau sebagian secara moderat. Kemudian diketahui terdapat risiko yang memiliki tingkat keparahan tertinggi sebesar 7, yaitu kerusakan data pada *database*. Nilai 7 tersebut menghasilkan dampak yang major atau menimbulkan ketidakpuasan pelanggan secara ektrim.

4. Penyebab Kegagalan Potensial

Potensi kegagalan yang muncul pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer memiliki beberapa penyebab, diantaranya:

a. *Human error*
   Human error merupakan kesalahan yang dilakukan oleh seseorang atau kelompok yang ada di dalam organisasi maupun perusahaan. Kesalahan tersebut dapat dilakukan baik sengaja maupun tidak sengaja dan berpotensi mengakibatkan kerugian.
b. Listrik mati

Kurangnya atau hilangnya pasokan listrik yang dapat berasal dari kesalahan teknisi maupun pemadaman yang dilakukan oleh pihak PLN (Perusahaan Listrik Negara). Hal ini mengakibatkan organisasi tidak mendapat pasokan listrik sehingga mengganggu jalannya proses bisnis yang didukung oleh tenaga listrik.

c. Serangan *hacker*
Keberadaan *hacker* yang melakukan serangan pada jaringan dapat memberikan dampak yang siginifikan dan mudah dirasakan. Jaringan yang terdampak akan secara langsung mengalami penurunan daya sehingga menimbulkan terganggunya proses bisnis. Akibatnya baik staf, dosen dan mahasiswa tidak dapat menjalankan tugas dan fungsi mereka sebagaimana mestinya.

d. Bencana alam
Bencana alam yang muncul pada iklim-iklim tertentu seperti musim hujan terkadang memberikan dampak yang cukup signifikan bagi organisasi. Bencana seperti hujan deras dan petir dapat memberikan kerugian ketika menimbulkan masuknya air pada ruang kerja dan rusaknya beberapa infrastruktur yang dimiliki.

Berikut ini merupakan penyebab munculnya potensi mode kegagalan yang ada pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer sesuai dengan hasil wawancara yang dilakukan pada beberapa pihak terkait:

1. Data pada *database* tidak valid
   a. *Human error*
   b. Listrik mati
   c. Lupa *log out*
   d. Orang tidak bertanggung jawab
2. Jaringan terganggu karena gangguan dari internal
   a. Serangan *hacker*
   b. Praktikum mata kuliah jaringan
3. *Workstation* jaringan mengalami gangguan akibat *brute force attack*
   a. Serangan *hacker*
4. *Mouse* rusak
   a. *Human error*
   b. Orang tidak bertanggung jawab
5. Jaringan terganggu karena penumpukan paket di *router*
   a. *Human error*
   b. Masalah *router*
   c. Listrik mati
6. Layanan MySQL terputus
   a. Listrik mati
   b. Kurangnya perawatan yang dilakukan (*maintenance*)
7. *Hardisk* penuh
   a. Data dan file ganda atau duplikat
   b. Data dan file tidak penting

c. *Human error*

8. *Hardisk master* dan *slave* rusak
   a. *Human error*
   b. Tidak dirawat dengan baik
9. Komputer rusak karena *power supply*
   a. *Human error*
   b. Listrik mati
10. Ruang kerja bocor dan kebanjiran
    a. *Human error*
    b. Bencana alam
11. Jaringan internet melambat karena *router* dan *access point* mati akibat petir
    a. Listrik mati
    b. Bencana alam

5. Menentukan Tingkat Probabilitas Kejadian (*Occurence*)

Di bawah ini merupakan hasil penilaian tingkat probabilitas kejadian (*occurence*) berdasarkan hasil analisis dari setiap potensi mode kegagalan yang ada pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer. Penilaian tersebut didasarkan pada kriteria penilaian yang dimiliki oleh tingkat probabilitas kejadian (*occurence*) dan didapatkan hasil sebagai berikut:

Tabel 4.39 Tingkat Probabilitas Kejadian (*Occurence*)

No.	Potensi Kegagalan	Penyebab	Tingkat Probabilitas
1.	Data pada *database* tidak valid	*Human error*	7
		Listrik mati	3
		Lupa *log out*	3
		Orang tidak bertanggung jawab	2
2.	Jaringan terganggu karena gangguan dari internal	Serangan *hacker*	8
		Praktikum mata kuliah jaringan	9
3.	*Workstation* jaringan mengalami gangguan akibat *brute force attack*	Serangan *hacker*	9
4.	*Mouse* rusak	Orang tidak bertanggung jawab	2
5.	Jaringan terganggu karena penumpukan paket di *router*	*Human error*	9

No.	Potensi Kegagalan	Penyebab	Tingkat Probabilitas
6.	Layanan MySQL terputus	Listrik mati	3
		Kurangnya perawatan (*maintenance*)	3
7.	*Hardisk* penuh	Data dan file ganda atau duplikat	4
		Data dan file tidak penting	4
		Human error	3
8.	*Hardisk master* dan *slave* rusak	*Human error*	3
		Tidak dirawat dengan baik	4
9.	Komputer rusak karena *power supply*	*Human error*	3
		Listrik mati	4
10.	Ruang kerja bocor dan kebanjiran	*Human error*	4
		Bencana alam	4
11.	Jaringan internet melambat karena *router* dan *access point* mati akibat petir	Listrik mati	4
		Bencana alam	4

Dari penilaian diatas didapatkan hasil bahwa sebagian besar risiko yang telah teridentifikasi pada Unit Pengelolaan Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer memiliki nilai tingkat probabilitas kejadian sebesar 3 dan 4. Nilai 3 pada kriteria tingkat probabilitas kejadian berarti bahwa risiko tersebut hanya terjadi sekali dalam kurun waktu satu hingga tiga tahun, sedangkan nilai 4 berarti bahwa risiko tersebut hanya terjadi sekali dalam kurun waktu setahun. Kemudian diketahui terdapat risiko yang memiliki tingkat probabilitas tertinggi 8 dan 9. Nilai 9 pada kriteria tingkat probabilitas kejadian berarti bahwa risiko tersebut terjadi dalam kurun waktu sekali dalam satu minggu, sedangkan nilai 9 berarti bahwa risiko tersebut terjadi sekali setiap tiga hingga empat hari.

6. Evaluasi Pengendalian

Proses atau langkah evaluasi dan kontrol memungkinkan organisasi maupun perusahaan untuk mengidentifikasi, mengenali dan mengatasi penyebab potensi kegagalan. Apabila langkah evaluasi dan kontrol ini dilakukan, maka akan dapat dapat digunakan untuk mengurangi hingga menghilangkan kemungkinan terjadinya potensi kegagalan yang akan merugikan organisasi maupun perusahaan. Dibawah ini merupakan langkah-langkah yang telah

dilakukan oleh Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer sebagai bentuk langkah evaluasi dan kontrol terhadap penyebab potensi kegagalan:

Tabel 4.40 Evaluasi Pengendalian

No.	Potensi Kegagalan	Penyebab	Pengendalian
1.	Data pada *database* tidak valid	*Human error*	Akses terbatas
		Listrik mati	*UPS dan server backup*
		Lupa *log out*	Akses terbatas
		Orang tidak bertanggung jawab	Akses terbatas
2.	Jaringan terganggu karena gangguan dari internal	Serangan *hacker*	*Firewall*
		Praktikum mata kuliah jaringan	*Firewall*
3.	*Workstation* jaringan mengalami gangguan akibat *brute force attack*	Serangan *hacker*	*Firewall*
4.	*Mouse* rusak	Orang tidak bertanggung jawab	Teguran hingga sanksi
5.	Jaringan terganggu karena penumpukan paket di *router*	*Human error*	Pemberian sosialisasi atau arahan
6.	Layanan MySQL terputus	Listrik mati	*UPS dan server backup*
		Kurangnya perawatan (*maintenance*)	Jadwal *maintenance*
7.	*Hardisk* penuh	Data dan file ganda atau duplikat	Menghapus data ganda
		Data dan file tidak penting	Menghapus data tidak penting
		Human error	Pemberian sosialisasi atau arahan
8.	*Hardisk master* dan *slave* rusak	*Human error*	Pemberian sosialisasi atau arahan

No.	Potensi Kegagalan	Penyebab	Pengendalian
		Tidak dirawat dengan baik	Mengganti dengan *hardisk* cadangan
9.	Komputer rusak karena *power supply*	*Human error*	Pemberian sosialisasi atau arahan
		Listrik mati	Mengganti UPS dan mengganti PC
10.	Ruang kerja bocor dan kebanjiran	*Human error*	Pemberian sosialisasi atau arahan
		Bencana alam	Membersihkan ruangan
11.	Jaringan internet melambat karena *router* dan *access point* mati akibat petir	Listrik mati	*UPS dan server backup*
		Bencana alam	Mengganti *router* dan *access point*

7. Menentukan Tingkat Kemampuan Deteksi (*Detection*)

Di bawah ini merupakan hasil penilaian tingkat kemampuan deteksi (*detection*) berdasarkan hasil analisis dari setiap potensi mode kegagalan yang ada pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer. Penilaian tersebut didasarkan pada kriteria penilaian yang dimiliki oleh tingkat kemampuan deteksi (*detection*) dan didapatkan hasil sebagai berikut:

Tabel 4.41 Tingkat Kemampuan Deteksi (*Detection*)

No.	Potensi Kegagalan	Penyebab	Pengendalian	Tingkat Deteksi
1.	Data pada *database* tidak valid	*Human error*	Akses terbatas	5
		Listrik mati	*UPS dan server backup*	7
		Lupa *log out*	Akses terbatas	5
		Orang tidak bertanggung jawab	Akses terbatas	5
2.	Jaringan terganggu karena gangguan	Serangan *hacker*	*Firewall*	3
		Praktikum mata	*Firewall*	3

No.	Potensi Kegagalan	Penyebab	Pengendalian	Tingkat Deteksi
	dari internal	kuliah jaringan		
3.	*Workstation* jaringan mengalami gangguan akibat *brute force attack*	Serangan *hacker*	*Firewall*	3
4.	*Mouse* rusak	Orang tidak bertanggung jawab	Teguran hingga sanksi	5
5.	Jaringan terganggu karena penumpukan paket di *router*	*Human error*	Pemberian sosialisasi atau arahan	5
6.	Layanan MySQL terputus	Listrik mati	*UPS dan server backup*	7
		Kurangnya perawatan (*maintenance*)	Jadwal *maintenance*	5
7.	*Hardisk* penuh	Data dan file ganda atau duplikat	Menghapus data ganda	6
		Data dan file tidak penting	Menghapus data tidak penting	6
		Human error	Pemberian sosialisasi atau arahan	5
8.	*Hardisk master* dan *slave* rusak	*Human error*	Pemberian sosialisasi atau arahan	5
		Tidak dirawat dengan baik	Mengganti dengan *hardisk* cadangan	7
9.	Komputer rusak karena *power supply*	*Human error*	Pemberian sosialisasi atau arahan	5
		Listrik mati	Mengganti UPS dan mengganti PC	7
10.	Ruang kerja bocor	*Human error*	Pemberian	5

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

No.	Potensi Kegagalan	Penyebab	Pengendalian	Tingkat Deteksi
	dan kebanjiran		sosialisasi atau arahan	
		Bencana alam	Membersihkan ruangan	7
11.	Jaringan internet melambat karena *router* dan *access point* mati akibat petir	Listrik mati	*UPS dan server backup*	7
		Bencana alam	Mengganti *router* dan *access point*	7

Dari penilaian diatas didapatkan hasil bahwa sebagian besar risiko yang telah teridentifikasi pada Unit Pengelolaan Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer memiliki nilai tingkat kemampuan deteksi sebesar 5 dan 7. Nilai 5 pada kriteria tingkat kemampuan deteksi berarti bahwa risiko tersebut memiliki tingkat deteksi sedang atau metode deteksi yang digunakan memiliki kemungkinan sedang atau rata-rata dalam mendeteksi risiko tersebut, sedangkan nilai 7 berarti bahwa risiko tersebut memiliki tingkat deteksi sangat rendah atau metode deteksi yang digunakan memiliki kemampuan yang tidak handal dalam melakukan deteksi terhadap risiko tersebut dengan tepat waktu

Kemudian diketahui terdapat risiko yang memiliki tingkat kemampuan deteksi tertinggi yaitu 3. Nilai 3 pada kriteria tingkat kemampuan deteksi berarti bahwa risiko tersebut memiliki tingkat deteksi tinggi atau metode deteksi yang digunakan memiliki kemungkinan yang tinggi untuk dapat mendeteksi adanya risiko tersebut.

8. Menentukan Tingkat Prioritas Risiko (*Risk Priority Number*)

Setelah melakukan penilaian terhadap tingkat keparahan dampak (*severity*), tingkat probabilitas kejadian (*occurence*), dan tingkat kemampuan deteksi (*detection*), maka langkah selanjutnya adalah melakukan perhitungan terhadap tingkat prioritas risiko. Perhitungan RPN dilakukan dengan mengalikan masing-masing nilai yang telah didapatkan sebelumnya. Dari data perhitungan terhadap tingkat prioritas risiko (RPN) diatas maka dapat diperoleh urutan prioritas terjadinya kegagalan berdasarkan besarnya nilai yang dihasilkan seperti yang tertera pada tabel di bawah ini:

Tabel 4.42 Hasil Perhitungan Tingkat Prioritas Risiko (RPN)

No.	Potensi Kegagalan	Penyebab	RPN
1.	Data pada *database* tidak valid	*Human error*	245
2.	Jaringan terganggu karena penumpukan paket di *router*	*Human error*	225

No.	Potensi Kegagalan	Penyebab	RPN
3.	Jaringan internet melambat karena *router* dan *access point* mati akibat petir	Bencana alam	210
4.	*Hardisk master* dan *slave* rusak	*Human error*	168
5.	Komputer rusak karena *power supply*	*Human error*	168
6.	Jaringan internet melambat karena *router* dan *access point* mati akibat petir	Listrik Mati	168
7.	Kerusakan data pada *database*	Listrik Mati	147
8.	Ruang kerja bocor dan kebanjiran	*Human error*	140
9.	Ruang kerja bocor dan kebanjiran	Bencana alam	140
10.	Jaringan terganggu karena gangguan dari internal	Praktikum mata kuliah jaringan	135
11.	Jaringan terganggu karena gangguan dari internal	Serangan *hacker*	120
12.	Layanan MySQL terputus	Kurangnya perawatan (*maintenance*)	120
13.	*Hardisk* penuh	Data dan file ganda atau duplikat	120
14.	Komputer rusak karena *power supply*	Listrik Mati	120
15.	Kerusakan data pada *database*	Lupa *log out*	105
16.	*Hardisk master* dan *slave* rusak	Kurangnya perawatan (*maintenance*)	90
17.	Layanan MySQL terputus	Listrik Mati	75
18.	*Hardisk* penuh	Data dan file tidak penting	75
19.	*Hardisk* penuh	*Human error*	75
20.	Kerusakan data pada *database*	Orang tidak bertanggung jawab	70
21.	*Workstation* jaringan mengalami gangguan akibat *brute force*	Serangan *hacker*	54

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

No.	Potensi Kegagalan	Penyebab	RPN
	attack		
22.	*Mouse* rusak	Orang tidak bertanggung jawab	40

Dari hasil perhitungan diatas, sesuai dengan kriteria yang dimiliki oleh tingkat prioritas risiko diketahui terdapat empat risiko yang memiliki status tingkat risiko sangat tinggi karena memiliki nilai lebih dari 200, tujuh risiko yang memiliki status tingkat risiko tinggi karena memiliki nilai kurang dari 200, enam risiko yang memiliki status tingkat risiko sedang karena memiliki nilai kurang dari 120, dan enam risiko yang memiliki status tingkat risiko rendah karena memiliki nilai kurang dari 80.

9. Mengidentifikasi Potensi Kegagalan Berdasarkan Praktik Keamanan

Setelah melakukan wawancara dan analisis dengan menggunakan kerangka kerja OCTAVE-S dan metode FMEA serta mendapatkan hasil dari masing-masing metode tersebut, maka langkah selanjutnya adalah menggabungkan kedua hasil yang diperoleh serta melakukan analisis. 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.

Pada analisis ini akan diketahui apakah setiap potensi kegagalan atau risiko yang teridentifikasi dengan menggunakan kerangka kerja OCTAVE-S serta kemudian dinilai dan diukur dengan menggunakan metode FMEA akan sesuai dengan masing-masing pernyataan praktik keamanan yang terdapat dalam kerangka kerja OCTAVE-S itu sendiri. Selain itu, analisis ini akan membantu untuk mengetahui apakah hasil penilaian atau pengukuran tingkat prioritas risiko dengan menggunakan metode FMEA akan sesuai dengan hasil penilaian praktik keamanan yang ada di dalam kerangka kerja OCTAVE-S. Berikut ini merupakan hasil dari analisis kesesuaian antara kerangka kerja OCTAVE-S dengan metode FMEA:

Tabel 4.43 Potensi Kegagalan Berdasarkan Praktik Keamanan

No.	Area Praktik Keamanan	Potensi Kegagalan	Penyebab
1.	Pengendalian Akses Fisik	*Mouse* rusak	Orang tidak bertanggung jawab
		Ruang kerja bocor dan kebanjiran	*Human error*
			Bencana alam
2.	Autentikasi dan Otorisasi	Data pada *database* tidak valid	*Human error*
			Listrik mati

No.	Area Praktik Keamanan	Potensi Kegagalan	Penyebab
			Lupa *log out*
			Orang tidak bertanggung jawab
		Jaringan terganggu karena penumpukan paket di *router*	*Human error*
		Jaringan terganggu karena gangguan dari internal	Serangan *hacker*
			Praktikum mata kuliah jaringan
3.	Manajemen Kerentanan	*Hardisk* penuh	Data dan file ganda atau duplikat
			Data dan file tidak penting
			Human error
		Hardisk master dan *slave* rusak	*Human error*
			Tidak dirawat dengan baik
		Data pada *database* tidak valid	*Human error*
			Listrik mati
			Lupa *log out*
			Orang tidak bertanggung jawab
		Jaringan terganggu karena gangguan dari internal	Serangan *hacker*
			Praktikum mata kuliah jaringan
		Workstation jaringan mengalami gangguan akibat *brute force attack*	Serangan *hacker*
		Mouse rusak	Orang tidak bertanggung jawab
		Komputer rusak karena *power supply*	*Human error*
			Listrik mati
		Layanan MySQL terputus	Listrik mati
			Kurangnya perawatan

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

No.	Area Praktik Keamanan	Potensi Kegagalan	Penyebab
			(*maintenance*)
4.	Manajemen Insiden	*Mouse* rusak	Orang tidak bertanggung jawab
		Komputer rusak karena *power supply*	*Human error*
			Listrik mati
		Ruang kerja bocor dan kebanjiran	*Human error*
			Bencana alam
		Jaringan internet melambat karena *router* dan *access point* mati akibat petir	Listrik mati
			Orang tidak bertanggung jawab

Dari tabel diatas dapat diketahui beberapa risiko yang berhubungan dengan masing-masing area praktik keamanan diatas. Hal ini disebabkan oleh kurangnya penerapan praktik keamanan yang dilakukan oleh organisasi pada masing-masing area tersebut. Risiko yang terdapat pada area pengendalian akses fisik diantaranya *mouse* rusak dan ruang kerja bocor dan kebanjiran. Risiko yang terdapat pada area autentikasi dan otorisasi diantaranya Kerusakan data pada *database,* jaringan terganggu karena penumpukan paket di *router,* dan jaringan terganggu karena gangguan dari internal. Risiko yang terdapat pada area manajemen kerentanan diantaranya *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*, dan layanan MySQL terputus. Dan risiko yang terdapat pada area manajemen insiden diantaranya *mouse* rusak, komputer rusak karena *power supply*, ruang kerja bocor dan kebanjiran, serta jaringan internet melambat karena *router* dan *access point* mati akibat petir.

4.2.3.3 Proses 5 - Mengembangkan Strategi Perlindungan dan Rencana Mitigasi

1. **Strategi Perlindungan Saat Ini**

Tabel 4.44 Strategi Perlindungan Aspek Keamanan

No.	Aspek Keamanan	*Stoplight*
1.	Pengendalian Akses Fisik	Kuning
2.	Autentikasi dan Otorisasi	Kuning
3.	Manajemen Kerentanan	Kuning
4.	Manajemen Insiden	Merah

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.

Area-area tersebut dipilih karena beberapa alasan. Area Pengendalian Akses Fisik dipilih karena tidak adanya dokumentasi perencanaan dan prosedur keamanan fasilitas yang digunakan untuk menjaga tempat, bangunan, dan setiap area yang terlarang. Kebutuhan fasilitas hanya didasarkan pada referensi atau standar yang diberlakukan secara umum. Selain itu PSIK juga tidak memiliki kebijakan dan prosedur yang terdokumentasi secara tertulis untuk mengelola pengunjung aset fisik serta pengunjung akses pada perangkat keras maupun lunak, namun hanya orang-orang tertentu saja yang dapat mengunjungi ataupun mengakses informasi penting secara fisik dari perangkat-perangkat tersebut.

Area Autentikasi dan Otorisasi dipilih karena seluruh kontrol akses pengguna tidak diatur langsung oleh PSIK namun dari kebijakan UPT TIK Universitas Brawijaya sebagai pusat teknologi Informasi pada Universitas Brawijaya. Sehingga proses penetapan dan penghentian hak akses pengguna diatur langsung oleh UPT TIK Universitas Brawijaya. Kemudian area Manajemen Kerentanan dipilih karena PSIK masih belum memiliki prosedur yang tertulis dengan jelas mengenai manajemen kerentanan organisasi. Prosedur manajemen kerentanan yang berlaku berasal dari UPT TIK Universitas Brawijaya yang kemudian diikuti oleh seluruh unit TIK fakultas di seluruh universitas. Selanjutnya UPT TIK Universitas Brawijaya akan melakukan pelatihan mengenai manajemen kerentanan kepada seluruh unit TIK dibawahnya yang kemudian akan dilaksanakan pada fakultas masing-masing.

Sedangkan area praktik keamanan Manajemen Insiden dipilih karena saat ini PSIK masih belum memiliki prosedur manajemen insiden yang dapat diuji, diverifikasi, dan diperbarui secara berkala. Serta masih belum memiliki kebijakan

dan prosedur yang terdokumentasi untuk bekerja dengan lembaga penegak hukum untuk mengatasi ancaman risiko yang terjadi.

2. Pendekatan Mitigasi

Berdasarkan hasil penilaian status *stoplight* yang terdapat pada lembar kerja profil risiko, dapat diketahui beberapa warna *stoplight* untuk masing-masing area praktik keamanan yang menunjukkan sejauh mana pelaksanaan praktik keamanan telah dijalankan di dalam organisasi. Pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer, area praktik keamanan yang memiliki status kuning adalah Pengendalian Akses Fisik, Autentikasi dan Otorisasi, dan Manajemen Kerentanan. Sedangkan area praktik keamanan yang memiliki status merah adalah Manajemen Insiden.

Status *stoplight* berwarna kuning ini berarti organisasi masih belum sepenuhnya sempurna dalam menerapkan praktik kemanan yang ada. Warna kuning juga dapat diartikan bahwa organisasi telah melaksanakan praktik keamanan namun hanya sampai pada batas tertentu, sehingga membutuhkan beberapa perbaikan. Sedangkan status merah ini berarti organisasi belum menerapkan praktik keamanan yang sesuai pada area tersebut atau praktik yang telah dilakukan masih buruk sehingga membutuhkan perubahan berupa perbaikan yang signifikan. Maka dari itu penulis memutuskan untuk melakukan mitigasi terhadap area yang berwarna kuning dan merah.

3. Rencana Mitigasi Risiko

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.

4. Perubahan Strategi Perlindungan

Selanjutnya memberikan rekomendasi mengenai langkah mitigasi yang harus dilakukan oleh organisasi pada setiap bidang area praktik keamanan yang telah dijelaskan sebelumnya.

b. Pengendalian Akses Fisik

Perubahan yang diperlukan pada area praktik keamanan ini adalah mendokumentasikan prosedur keamanan fasilitas secara resmi untuk melindungi tempat dan area terlarang. Selain itu juga mendokumentasikan kebijakan dan prosedur untuk melindungi media perangkat keras maupun lunak. Kedua prosedur tersebut digunakan untuk melindungi aset dari akses pengunjunjung secara fisik yang tidak sah. Selain itu melakukan penataan atau pengaturan ulang terhadap ruang kerja untuk membatasi akses fisik pada infrastruktur komputer baik perangkat keras maupun lunak. Serta menyediakan atau memberikan pelatihan kepada seluruh karyawan

tentang pengendalian akses fisik untuk mengelola akses pada tempat kerja maupun infrastruktur komputer.

c. Autentikasi dan Otorisasi
   Perubahan yang diperlukan pada area praktik keamanan ini adalah mendokumentasikan mekanisme yang digunakan untuk memastikan perlindungan terhadap informasi penting yang dimiliki oleh organisasi. Mekanisme tersebut digunakan untuk memastikan bahwa informasi yang dimiliki tidak dapat diubah maupun dihilangkan melalui akses yang tidak sah.
d. Manajemen Kerentanan
   Perubahan yang diperlukan pada area praktik keamanan ini adalah mendokumentasikan prosedur manajemen kerentanan secara resmi yang sesuai dengan kondisi terkini dari organisasi. Kemudian melakukan audit keamanan teknologi informasi secara berkala untuk mengidentifikasi kelemahan keamanan di dalam infrastruktur komputasi. Serta menyediakan atau memberikan pelatihan manajemen kerentanan kepada seluruh karyawan.
e. Manajemen Insiden
   Perubahan yang diperlukan pada area praktik keamanan ini adalah mendokumentasikan prosedur manajemen insiden secara resmi, kemudian melakukan pengujian terhadap dokumen prosedur manajemen insiden secara berkala untuk memastikan kesesuaian dengan kondisi terkini dari organisasi. Serta menyediakan atau memberikan pelatihan manajemen insiden kepada seluruh karyawan.

5. Identifikasi Langkah Selanjutnya

Untuk mendukung peningkatan keamanan, keamanan informasi harus menjadi prioritas bagi Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer. Sebagai sebuah prioritas pada tingkat strategis, maka organisasi juga harus mampu mengalokasikan dana untuk mendukung pelaksanaan implementasi rencana mitigasi. Kemudian memastikan bahwa seluruh pihak turut menjalankan kebijakan yang telah dibuat dengan maksimal. Serta kepala bagian harus memastikan bahwa seluruh karyawannya dapat berpartisipasi dalam segala aktivitas yang berkaitan dengan keamanan seperti pelatihan dan lain sebagainya.

Pemantauan pelaksanaan implementasi dapat dilakukan dengan berbagai cara, diantaranya:

a. Melakukan pemantauan terhadap kinerja karyawan yang dilakukan secara berkala.
b. Mewajibkan untuk membuat laporan status bulanan kepada Kepala Unit.
c. Melaksanakan evaluasi melalui rapat yang dilakukan setiap bulan dan melakukan pemeriksaan terhadap laporan secara rutin.

Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer tidak akan melakukan perluasan untuk penambahan aset kritis yang

dimiliki apabila kegiatan mitigasi yang ada saat ini belum diterapkan secara menyeluruh di dalam organisasi. Penulis menganjurkan pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer untuk melakukan pengukuran risiko keamanan informasi selanjutnya dengan menggunakan metode OCTAVE-S setiap satu tahun sekali.

BAB 5 PEMBAHASAN

OCTAVE-S memiliki beberapa area praktik keamanan yang harus di laksanakan oleh organisasi untuk memastikan strategi perlindungan organisasi yang luas. Hasil penilaian yang dilakukan akan menunjukkan sejauh mana organisasi telah mengikuti praktik keamanan yang baik. Berdasarkan hasil evaluasi terhadap pelaksanaan praktik keamanan pada unit PSIK telah didapatkan dan diketahui beberapa area yang dinilai masih kurang baik sehingga membutuhkan perbaikan. Area-area tersebut adalah area yang memiliki status *stoplight* kuning dan merah. Selanjutnya diberikan rekomendasi langkah-langkah mitigasi untuk memperbaiki praktik yang telah dilakukan pada area-area praktik keamanan tersebut.

5.1 Pengendalian Akses Fisik

Area praktik keamanan pengendalian akses fisik mendapatkan status *stoplight* kuning yang artinya organisasi masih belum sepenuhnya sempurna atau baik dalam menerapkan praktik keamanan pada area ini. Status *stoplight* kuning tersebut juga dapat diartikan bahwa organisasi hanya menerapkan sedikit atau hanya sebagian dari keseluruhan praktik keamanan pada area tersebut sehingga masih membutuhkan beberapa perbaikan. Untuk mendapatkan status *stoplight* hijau maka organisasi harus melakukan beberapa langkah penanganan pada area praktik keamanan tersebut diantaranya, membuat dokumen rencana dan prosedur keamanan fasilitas secara resmi yang dapat diuji. Hal ini berfungsi untuk menjaga dan melindungi tempat, bangunan dan setiap area yang dinilai terlarang untuk diakses secara umum. Kemudian membuat kebijakan dan prosedur untuk melakukan pengelolaan terhadap pengunjung aset fisik secara resmi. Membuat kebijakan dan prosedur untuk melakukan kontrol terhadap akses fisik, baik pada media perangkat keras maupun lunak secara resmi. Hal ini berfungsi untuk membantu mengidentifikasi dan mengelola siapa saja yang bertanggung jawab untuk melakukan kontrol secara berkala terhadap seluruh aset. Melakukan pengujian secara berkala terhadap dokumen-dokumen resmi yang berkaitan dengan praktik pengendalian akses fisik. Hal ini berfungsi untuk memastikan kesesuaian dokumen-dokumen yang dimiliki dengan keadaan terkini organisasi sehingga dokumen tersebut akan dapat dipastikan relevansinya.

Selanjutnya mengatur ulang kantor atau ruang kerja untuk membatasi akses fisik ke sistem, komputer, atau perangkat lain oleh personel yang tidak sah. Seperti yang diketahui bahwa keadaan ruang kerja PSIK sangat berbahaya bagi siapapun yang masuk karena tata letak infrastruktur yang masih tidak teratur. Penataan ulang kembali terhadap ruang kerja akan membantu melindungi seluruh infrastruktur komputer dari akses-akses yang tidak sah dan rentan baik yang dilakukan secara sengaja maupun tidak. Mempertahankan layanan penjaga keamanan untuk melindungi tempat, bangunan, ruang kerja serta seluruh infrastruktur. Hal ini dapat dilakukan dengan melakukan kerjasama dengan pihak keamanan universitas. Serta 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. Pelatihan yang diberikan kepada seluruh karyawan akan membantu melatih kesiapan mereka jika sewaktu-waktu dibutuhkan. Dengan memberikan pelatihan tersebut karyawan akan mengetahui langkah-langkah yang harus dilakukan ketika menghadapi permasalahan terkait dengan kendali terhadap akses fisik.

5.2 Autentikasi dan Otorisasi

Area praktik keamanan autentikasi dan otorisasi mendapatkan status *stoplight* kuning yang artinya organisasi masih belum sepenuhnya sempurna atau baik dalam menerapkan praktik keamanan pada area ini. Status *stoplight* kuning tersebut juga dapat diartikan bahwa organisasi hanya menerapkan sedikit atau hanya sebagian dari keseluruhan praktik keamanan pada area tersebut sehingga masih membutuhkan beberapa perbaikan. Untuk mendapatkan status *stoplight* hijau maka organisasi harus melakukan beberapa langkah penanganan pada area praktik keamanan tersebut diantaranya, 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. Hal ini berfungsi untuk memastikan kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) dari informasi itu sendiri ketika dibutuhkan dan diakses oleh pengguna kapan saja. Kemudian melakukan pengujian secara berkala terhadap mekanisme perlindungan informasi yang telah dibuat. Pengujian yang dibuat berfungsi untuk memastikan kesesuaian dokumen-dokumen yang dimiliki dengan keadaan terkini organisasi sehingga dokumen tersebut akan dapat dipastikan relevansinya.

5.3 Manajemen Kerentanan

Area praktik keamanan manajemen kerentanan mendapatkan status *stoplight* kuning yang artinya organisasi masih belum sepenuhnya sempurna atau baik dalam menerapkan praktik keamanan pada area ini. Status kuning tersebut juga dapat diartikan bahwa organisasi hanya menerapkan sedikit atau hanya sebagian dari keseluruhan praktik keamanan pada area tersebut sehingga masih membutuhkan beberapa perbaikan. Untuk mendapatkan status *stoplight* hijau maka organisasi harus melakukan beberapa langkah penanganan pada area praktik keamanan tersebut diantaranya, membuat prosedur secara tertulis dan resmi serta dapat diuji untuk mengelola tingkat kerentanan. Prosedur yang dibuat akan membantu organisasi dalam mengelola kerentanan (*vulnerability*) seperti memilih alat (*tools*) evaluasi kerentanan yang sesuai untuk digunakan, mengidentifikasi komponen infrastruktur yang akan dievaluasi, menjadwalkan pelaksanaan evaluasi kerentanan, hingga menanggapi hasil evaluasi yang akan didapatkan. Selain itu juga menjaga keamanan media penyimpanan yang digunakan dan menghilangkan data yang dinilai rentan. Prosedur manajemen kerentanan juga dapat membantu organisasi untuk tetap *up to date* terhadap jenis kerentanan yang telah diketahui beserta dengan metode penyerangannya.

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Kemudian melakukan pengujian secara berkala terhadap prosedur kerentanan untuk memastikan kesesuaian dokumen dengan keadaan terkini dari organisasi. Pengujian yang dibuat berfungsi untuk memastikan kesesuaian dokumen-dokumen yang dimiliki dengan keadaan terkini organisasi sehingga dokumen tersebut akan dapat dipastikan relevansinya. Selanjutnya melakukan audit keamanan teknologi informasi untuk mengidentifikasi kelemahan keamanan di dalam infrastruktur komputasi. Ini merupakan hal yang penting karena dengan audit yang dilakukan secara berkala maka akan membantu organisasi untuk mengetahui celah kelemahan mereka dengan cepat sehingga kemudian kelemahan itu dapat segera diatasi agar tidak menimbulkan risiko lain lebih lanjut. Serta memberikan atau menyediakan pelatihan manajemen kerentanan kepada seluruh karyawan. Pelatihan yang diberikan kepada seluruh karyawan akan membantu melatih kesiapan mereka jika sewaktu-waktu dibutuhkan. Dengan memberikan pelatihan tersebut karyawan akan mengetahui langkah-langkah yang harus dilakukan ketika menghadapi permasalahan terkait dengan manajemen kerentanan.

5.4 Manajemen Insiden

Area praktik keamanan manajemen insiden mendapatkan status *stoplight* merah yang artinya organisasi masih buruk dalam menerapkan praktik keamanan pada area ini. Status merah tersebut juga dapat diartikan bahwa organisasi belum menerapkan praktik keamanan apapun dari keseluruhan praktik keamanan pada area tersebut sehingga membutuhkan perbaikan yang signifikan. Untuk mendapatkan status *stoplight* hijau maka organisasi harus melakukan beberapa langkah penanganan pada area praktik keamanan tersebut diantaranya, membuat prosedur manajemen insiden secara resmi yang dapat diuji dan diverifikasi. Pembuatan prosedur ini berfungsi untuk membantu organisasi dalam menerapkan manajemen insiden yang sesuai dengan standar yang berlaku seperti melakukan identifikasi, melaporkan dan memberikan tanggapan tentang adanya dugaan insiden keamanan serta pelanggaran yang terjadi pada organisasi.

Kemudian melakukan pengujian secara berkala terhadap dokumen prosedur manajemen insiden. Hal ini berfungsi untuk memastikan kesesuaian dokumen tersebut dengan keadaan terkini dari organisasi sehingga dokumen tersebut akan dapat dipastikan relevansinya. Serta memberikan atau menyediakan pelatihan manajemen insiden kepada seluruh karyawan. Pelatihan yang diberikan kepada seluruh karyawan akan membantu melatih kesiapan mereka jika sewaktu-waktu dibutuhkan. Dengan memberikan pelatihan tersebut karyawan akan mengetahui langkah-langkah yang harus dilakukan ketika menghadapi permasalahan terkait dengan manajemen insiden.

BAB 6 PENUTUP

6.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis yang dilakukan pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer Universitas Brawijaya, maka dapat diambil kesimpulan sebagai berikut:

1. Aset-aset kritis yang teridentifikasi pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer antara lain FILKOM Apps yang merupakan sebuah sistem informasi yang terintegrasi dengan seluruh proses bisnis yang ada pada Fakultas Ilmu Komputer dan digunakan untuk mengelola data dan informasi yang dimiliki; serta Infrastruktur Data dan Jaringan yang merupakan sarana penunjang berjalannya seluruh sistem dan jaringan yang ada.
2. Analisis risiko teknologi informasi dilakukan dengan menggunakan kerangka kerja OCTAVE-S di mana kerangka kerja tersebut berfokus kepada risiko organisasi, hasil praktik dan strategi keamanan yang saling berkaitan. Hasil dari analisis risiko yang dilakukan pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer menunjukkan bahwa dari lima belas area praktik keamanan yang disediakan oleh kerangka kerja OCTAVE-S, terdapat tiga area praktik keamanan yang memiliki status *stoplight* kuning dan satu area praktik keamanan yang memiliki status *stoplight* berwarna merah. Area praktik keamanan yang berstatus *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. Untuk mencapai status *stoplight* hijau, maka diberikan rekomendasi langkah-langkah mitigasi sebagai berikut
   a. Pada area praktik keamanan Pengendalian Akses Fisik untuk mencapai status *stoplight* berwarna hijau maka organisasi perlu membuat rencana dan prosedur keamanan fasilitas secara resmi untuk menjaga bangunan dan area yang terlarang untuk umum, membuat kebijakan dan prosedur untuk pengelolaan pengunjung aset fisik, melakukan akses kontrol terhadap akses fisik, baik pada media perangkat keras maupun lunak, melakukan pengujian terhadap dokumen-dokumen resmi yang berkaitan dengan praktik pengendalian akses fisik secara berkala, mengatur ulang kantor atau ruang kerja, bekerja sama dengan petugas keamanan, serta memberikan atau menyediakan pelatihan kepada karyawan.

b. Pada area praktik keamanan Autentikasi dan Otorisasi untuk mencapai status *stoplight* berwarna hijau maka organisasi perlu membuat dan menyediakan mekanisme formal untuk memastikan keamanan dan ketersediaan informasi penting serta melakukan pengujian terhadap mekanisme perlindungan informasi secara berkala.
c. Pada area praktik keamanan Manajemen Kerentanan untuk mencapai status *stoplight* berwarna hijau maka organisasi perlu membuat prosedur resmi untuk mengelola tingkat kerentanan, melakukan pengujian secara berkala terhadap prosedur kerentanan, melakukan audit keamanan teknologi informasi, serta memberikan atau menyediakan pelatihan manajemen kerentanan kepada seluruh karyawan.
d. Pada area praktik keamanan Manajemen Insiden untuk mencapai status *stoplight* berwarna hijau maka organisasi perlu membuat prosedur manajemen insiden secara resmi, melakukan pengujian secara berkala terhadap dokumen prosedur manajemen insiden, serta memberikan atau menyediakan pelatihan manajemen insiden kepada seluruh karyawan.

6.2 Saran

Berdasarkan penelitian yang telah dilakukan, maka diberikan beberapa saran yang dapat digunakan oleh organisasi sebagai berikut:

1. Seluruh karyawan dari Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer harus mengutamakan keamanan sistem, data dan informasi yang dimiliki. Seluruh karyawan harus dapat berpartisipasi dalam seluruh kegiatan yang berkaitan dengan manajemen keamanan dan menjalankan seluruh kebijakan dan prosedur yang telah dibuat oleh organisasi dengan maksimal.
2. Pihak manajerial harus melakukan pemantauan secara berkala terhadap kinerja karyawan, mengadakan rapat setiap bulannya sebagai langkah untuk melakukan evaluasi, melakukan pemeriksaan laporan secara berkala, serta melakukan dokumentasi terhadap setiap perkembangan sistem yang sedang dijalankan sebagai bahan untuk evaluasi.
3. Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer disarankan untuk membuat kebijakan keamanan penggunaan teknologi informasi yang terdokumentasi secara resmi dan dapat diverifikasi. Hal ini bertujuan agar seluruh karyawan dapat ikut bertanggung jawab dalam hal menjaga keamanan internal organisasi.
4. Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer disarankan untuk melakukan evaluasi risiko teknologi informasi dengan menggunakan kerangka kerja OCTAVE-S setiap satu tahun sekali agar dapat mengantisipasi dan meminimalisir

kemungkinan terjadinya risiko yang muncul setiap tahunnya. Sehingga organisasi dapat terus melakukan pengembangan manajemen teknologi informasi, meningkatkan kualitas serta menjaga keberlangsungan proses bisnis yang dimiliki.

5. Selanjutnya penilaian risiko juga dilakukan pada aset orang di mana dapat berpotensi memunculkan risiko berupa hilangnya orang atau personil tertentu dari organisasi yang memiliki tugas, fungsi dan kemampuan yang tidak dapat digantikan oleh orang lain.

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.

Charette, R. 1989. *Software Engineering Risk Analysis and Management.* New York: McGraw-Hill.

Committe, J. T. 2004. *AS/NZS 4360:2004 Risk Management.* New Zealand: Standards Australia International Ltd.

Committee, J. T. 1999. *AS/NZS 4360:1999 Risk Management.* Strathfield: Standards Association of Australia.

Djohanputro, B. 2008. *Manajemen Risiko Korporat.* Jakarta: PT Karisma Teknika Citeurep.

Gelinas, U. J., Dull, R. B., & Wheeler, P. R. 2012. *Accounting Information Systems: Foundations in Enterprise Risk Management 9th edition*. Canada: Cengage Learning

Gondodiyoto, S. 2007. *Audit Sistem Informasi Lanjutan + Standar, Panduan, Prosedur Audit SI dari ISACA. Edisi Pertama*. Jakarta: Mitra Wacana Media.

Gondodiyoto, S. 2009. *Pengelolaan Fungsi Audit Sistem Informasi. Edisi Kedua*. Jakarta: Mitra Wacana Media.

Gunawan, B. M. 2011. *Information Technology Risk Assessment: Octave-S Approach*. CommIT.

Hanafi, M. M. 2016. *Manajemen Risiko.* Yogyakarta: Penerbit UPP STIM YKPN.

Harahap, R. M. 2011. *Information Technology Risk Measurement: Octave-S Method*. CommIT.

Hidayat, M. 2011. *Manajemen Aset (Privat dan Publik).* Yogyakarta: LaksBang.

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

Indrajit, R. E. 2000. *PENGANTAR KONSEP DASAR: MANAJEMEN SISTEM INFORMASI DAN TEKNOLOGI INFORMASI*. Jakarta: PT Elex Media Komputindo.

Jogiyanto, H. 1999. *Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis.* Yogyakarta: ANDI Yogyakarta.

Jogiyanto, H. 2007. *Metode Penelitian Bisnis: Salah Kaprah dan Pengalaman-Pengalaman.* Yogyakarta: BPFE.

repository.ub.ac.id
UNIVERSITAS BRAWIJAYA

Jordan, E., & Silcock, L. 2005. *Beating It Risks.* New York: John Wiley & Sons, Inc.

Kelvin., Jaya, K. & Effendi, P. H., 2012. *Pengukuran Risiko Teknologi Informasi Dengan Pendekatan OCTAVE-S pada PT. Mandala Multifinance, TBK*. S1. Universitas Bina Nusantara.

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

Martin, E. 1999. *Managing Information Technology What Managers Need to Know (3rd ed.).* New Jersey: Pearson Education International.

Martono, A. H. 2012. *Manajemen Keuangan. Edisi ke-2.* Yogyakarta: Ekonisia.

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

Mcleod, J. R. & Schell, G. 2001. *Management Information System. Edisi ke-8.* New Jersey: Prentice Hall.

Munawir, S. 2007. *Analisa Laporan Keuangan. Edisi Keempat.* Yogyakarta: Liberty.

O'Brien, J. A., & Marakas, G. M. 2002. *Introduction to Information Systems, Edisi ke-16*. New York: McGraw Hill.

O'Brien, J. A., & Marakas, G. M. 2006. *Management Information System, Edisi ke-7*. New York: McGraw Hill.

O'Brien, J. A., & Marakas, G. M. 2007. *Management Information Systems, Edisi ke-7.* New York: McGraw-Hill.

Ouertani, M. Z., Parlikad, A. K. & McFarlane, D. 2008. Towards An Approach to Select An Asset Information Management Strategy. *International Journal of Computer Science and Applications*, Halaman 25-44.

Peraturan Rektor Universitas Brawijaya Nomor 20 Tahun 2016 Tentang Susunan Organisasi dan Tata Kerja. Malang: Rektor Universitas Brawijaya.

Priandoyo, A. 2006. *Vulnerability Assessment untuk Meningkatkan*. Jurnal Sistem Informasi, 73-83.

Rainer Jr, R. K. 2013. *Introduction to Information Systems- fourth edition.* Singapore: John Wiley and Sons Singapore pte. Ltd.

Rhasyid, A., Septiani, C. & Listianty, T., 2012. *Pengukuran Risiko Teknologi Informasi pada Rumah Sakit Bhakti Yudha Dengan Menggunakan Metode OCTAVE-S*. S1. Universitas Bina Nusantara.

Ross, J.W., Beath, C.M. & Goodhue D.L., 1995. *Developing Long-term Competitiveness Through Information Technology Assets.* Cambridge: MIT Sloan School of Management Center for Information Systems Research Working Paper No. 290.

Sanjaya, T., Pastriyani, I. A. & Febianto, H., 2012. *Pengukuran Risiko Teknologi Informasi pada Kementerian Komunikasi Dan Informatika Dengan Metode OCTAVE-S*. S1. Universitas Bina Nusantara

Sopandi, D. 2008. *Instalasi dan Konfigurasi Jaringan Komputer*. Jakarta: Informatika.

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

Stephanus. 2014. *Implementation OCTAVE-S And ISO 27001 Controls In Risk Management Information Systems.* ComTech, 685-693.

Turban, E. & Volonino, L. 2012. *Information Technology for Management. 8th ed.* Hoboken: John Wiley & Sons.

Turban, E., Rainer, R. K., & Potter, E. 2003. *Introduction to Information Technology.* New York: John Wiley & Sons, Inc.

Turban, E., Rainer, R. K., & Potter, E. 2007. *Introduction to Information Systems: Supporting and Transforming Business.* New York: John Wiley & Sons, Inc.