ANALISIS DAN MITIGASI RISIKO ASET TI MENGGUNAKAN *FRAMEWORK* OCTAVE DAN FMEA (STUDI KASUS: POLTEKKES SEMARANG)

ANALYZATION AND RISK MITIGATION OF IT ASSET USING OCTAVE AND FMEA FRAMEWORK (CASE STUDY: POLTEKKES SEMARANG)

Melita Dyah Purwitasari[1], Wellia Shinta Sari, M.Kom[2]
Fakultas Ilmu Komputer, Universitas Dian Nuswantor Semarang
e-mail: [1]melita.dyah59@yahoo.com, [2]wellia_shinta@yahoo.com

Abstrak

Penerapan teknologi informasi pada institusi perguruan tinggi dalam membantu proses pengelolaan dan pengolahan informasi telah dilakukan oleh Politeknik Kesehatan Kemenkes Semarang, baik itu untuk mengelola data dan informasi yang berkaitan dengan civitas akademik terkait maupun data yang berkaitan dengan institusi. Hanya saja dengan segala kemudahan yang diperoleh, tidak dapat dipungkiri bahwa dalam pelaksanaannya pemanfaatan teknologi informasi memiliki beberapa risiko. Beberapa hal yang mungkin terjadi dalam proses yang berlangsung yaitu hilangnya data, redundancy, data rusak, infeksi data oleh malware dan virus, maupun personil yang menyalah gunakan hak akses yang dimiliki. Hal-hal tersebut tentunya akan menghambat proses bisnis dan merugikan baik itu dari segi waktu maupun biaya. Sehingga mitigasi risiko dilakukan dengan menggunakan bantuan dari metode OCTAVE dan FMEA sehingga tercipta suatu daftar risiko. Dan dengan menggunakan kontrol ISO 27002:2013 sebuah panduan penanggulangan untuk mengurangi atau bahkan menghilangkan risiko diterapkan.

Kata kunci*— mitigasi risiko, OCTAVE, FMEA, ISO 27002:2013, aset,teknologi informasi*

Abstract

The applications of information technology in higer education institutions in assisting the process of management and information processing has been carried out by Politeknik Kesehatan Kemenkes Semarang, wheter it is to manage data and information related to the academic community and the relevant data relating to the institution. It's just that with all the ease acquired, we can not denied that in actual utilization of information technologi has some risk. Some things that may occur to the process are the lost of data, dedudancy, corrupted data, data infection by malware and virus, or even a worker who misuse the privileges that they have. These things will certainly hamper the business process and detrimental both in term of time and cost. So that risk mitigation shall be done with the help of OCTAVE and FMEA methods to create a list of risk. And by using ISO 27002:2013 a guideline control to reduce or even remove the risk which about to happen is formed.

Keywords*— risk mitigation, OCTAVE, FMEA, ISO 27002:2013, asset, information technology*

1. PENDAHULUAN

Teknologi informasi merupakan salah satu faktor pendukung meningkatnya produktivitas proses bisnis dari suatu organisasi pada era globalisasi yang semakin berkembang pesat. Penerapan teknologi informasi tentunya harus diimbangi dengan pengelolaan yang juga memadai. Sama

halnya dengan penyedia layanan pendidikan yang memerlukan informasi sebagai pondasi keberhasilan kinerjanya. Penerapan teknologi informasi pada institusi perguruan tinggi dalam membantu proses pengelolaan dan pengolahan informasi telah dilakukan oleh Politeknik Kesehatan Kemenkes Semarang, baik itu untuk mengelola data dan informasi yang berkaitan dengan civitas akademik terkait maupun data yang berkaitan dengan institusi. Hanya saja dengan segala kemudahan yang diperoleh, tidak dapat dipungkiri bahwa dalam pelaksanaannya pemanfaatan teknologi informasi memiliki beberapa risiko.
Diperlukan kerjasama dari berbagai pihak terkait untuk menyusun prosedur dan penerapan kebijakan dari risiko teknologi informasi. Dengan menerapkan *framework* yang sesuai dengan kondisi yang diperlukan institusi membuat penyelesaian masalah menjadi lebih cepat dan tepat. Seperti penggunaan kerangka kerja *Operationally Critical Trait, Asset and Vunerabillity Evaluation* (OCTAVE) Metode OCTAVE merupakan teknik strategi dan perencanaan untuk keamanan atas risiko. Dan pemakaian prosedur *Failure Mode and Effect Analysis* (FMEA) untuk menilai risiko yang mungkin akan terjadi kedepan dengan mempersiapkan proses, desain maupun kendala dari risiko. Kemudian penerapan kontrol ISO 27002:2013 yang berisikan panduan atas penanganan risiko digunakan sebagai saran tindakan perbaikan.

2. METODE PENELITIAN

2.1 Metode Pengumpulan Data

1. Wawancara dengan pihak terkait

Wawancara merupakan metode pengumpulan data dengan cara bertanya langsung kepada responden terkait. Dalam penelitian ini, wawancara dilakukan dengan Kepala Bagian Divisi TI Politeknik Kesehatan Kemenkes Semarang.

2. Observasi

Merupakan metode pengumpulan data dengan cara melakukan pengamatan langsung untuk melihat dan merekam keadaan yang sesungguhnya.

3. Studi pustaka

Merupakan metode pengumpulan data dengan cara studi terhadap buku, literature, catatan maupun dokumen yang berhubungan dengan masalah yang dipecahkan.

2.2 Jenis Data

Data kualitatif, data ini merupakan metode yang menekankan pada aspek pemahaman mendalam terhadap suatu masalah. Dalam penelitian ini, data kualitatif diperoleh dari analisa dokumen, wawancara, observasi maupun diskusi dengan pihak terkait.

2.3 Sumber Data

1. Data Primer

Adalah data yang diperoleh langsung dari sumber asli atau pihak pertama. Dalam penelitian ini data primer didapat dari wawancara kepada pegawai dan observasi langsung ke institusi.

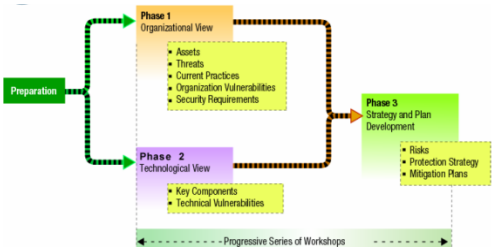
2. Data Sekunder

Adalah data yang diperoleh secara tidak langsung atau melalui perantara. Buku dan jurnal yang berkaitan dengan manajemen risiko, keamanan aset dan komponen teknologi informasi.

2.4 Metode Analisis

1. Metode OCTAVE digunakan untuk menjabarkan tingkatan risiko, daftar komponen risiko, dan bagaimana cara menanggulanginya.

Metode OCTAVE merupakan teknik strategi dan perencanaan untuk keamanan atas risiko.



Gambar 2.1 Fase OCTAVE [1]

Fase 1 : Membangun profil ancaman berlandaskan aset yang ada di organisasi
Tim analisis menentukan apa yang penting bagi organisasi dan apa yang saat ini sedang diterapkan dalam melindungi aset. Kemudian dipilih mana yang paling penting bagi organisasi (aset kritis) dan dideskripsikan kebutuhan keamanan, ancaman dan profil ancaman pada masing-masing aset kritis.
Fase 2 : Mengidentifikasi Kerentanan Infrastuktur/Teknologi
Adalah evaluasi atas informasi infrastruktur misal, mengidentifikasi kelas-kelas komponen teknologi informasi yang berkenaan dengan masing-masing aset kritis dan menentukan seberapa luas tiap komponen mampu bertahan atas serangan.
Fase 3 : Mengembangkan rencana dan strategi keamanan
Risiko atas aset kritis organisasi diidentifikasi dan ditentukan langkah yang harus diambil dalam menyikapinya. Strategi perlindungan diciptakan untuk organisasi dan rencana mitigasi ditambahkan untuk membantu pengelolaan risiko terhadap aset kritis berdasarkan analisa dari informasi yang telah dikumpulkan.

2. Metode FMEA digunakan untuk pemberian bobot atas peluang terjadinya kegagalan dalam sistem, proses, serta produk maupun servis untuk menentukan tingkat keseriusan efek yang ditimbulkan.

Metode *Failure and Effects Analysis* (FMEA) merupakan pendekatan secara sistematis untuk mengidentifikasi peluang terjadinya kegagalan dalam sistem, proses, serta produk maupun servis. *Failure Mode* berfokus pada langkah ataupun penggunaan mode yang memungkinkan terjadinya kegagalan, sedangkan *Effects Analysis* berfokus pada evaluasi yang membahas konsekuensi yang akan diterima dari kegagalan tersebut[2].

Tabel 2.1 Tahapan dalam FMEA [2]

Tahapan	Penjelasan
1. Memilih aset yang ingin dianalisa	Pilih aset dimana kesalahan sering terjadi
2. Urutkan dan pilih aset serta tim yang	Analisis aset yang perlu dilakukan penerapan FMEA dan orang-orang terkait aset tersebut.

Tahapan	Penjelasan
bertanggung jawab	
3. Jabarkan aset	Jabarkan secara lengkap mengenai aset yang akan dianalisa
4. Identifikasi kemungkinan terjadinya kesalahan pada masing-masing aset	Menjabarkan permasalahan yang mungkin terjadi pada tiap aset yang telah lebih dulu di pilih
5. Pilih permasalahan dengan risiko paling serius	Fokus pengembangan perbaikan atas permasalahan yang sering terjadi atau memiliki efek yang cukup besar bagi organisasi
6. Rancang dan implementasikan perubahan untuk mengurangi atau mencegah terjadinya masalah	Merencanakan rencana perbaikan atas risiko yang mungkin terjadi di kemudian hari untuk meminimalisisr atau bahkan menghilangkan risiko tersebut.
7. Ukur dan nilai keberhasilan perubahan aset	Mengevaluasi hasil dari penerapan perencanaan rencana perbaikan

Tahapan penilaian FMEA:

1. *Severity* (S): Tingkat keparahan, merupakan penilaian seberapa serius efek atas kegagalan yang berpotensial terjadi dari skala 1-10 dimana 1 adalah paling rendah.
2. *Occurence* (O): Keterjadian, seberapa sering terjadinya kegagalan pada suatu aset dari skala 1-10 dimana 1 adalah paling rendah.
3. *Detection* (D): Merupakan penilaian atas kemungkinan terdeteksinya penyebab terjadinya suatu bentuk kegagalan pada aset dari skala 1-10 dimana 1 adalah paling tinggi.
4. *Risk Priority Number* (RPN): Merupakan hasil prioritas risiko yang didapat dari pengalian *Severity*, *Occurence* dan *Detection* dengan rumus RPN= S x O x D.

Tabel 2.2 Nilai RPN [2]

Level	Nilai RPN
Very Low (Sangat Rendah)	0 sampai 20
Low (Rendah)	21 sampai 80
Moderate (Sedang)	81 sampai 120
High (Tinggi)	121 sampai 199
Very High (Sangat Tinggi)	Lebih dari 200

3. HASIL DAN PEMBAHASAN

3.1 Daftar Aset Kritis

Daftar Aset Kritis pada Politeknik Kesehatan Kemenkes Semarang yang didapat dari Kepala Unit Divisi IT yaitu sebagai berikut:

Tabel 3.1 Daftar Aset Kritis

Kelompok Aset	Aset Kritis	Penjelasan
Hardware	PC	Digunakan untuk menunjang proses bisnis utama.
	Router	Digunakan sebagai penghubung antar jaringan yang digunakan untuk meneruskan data dari jaringan yang satu ke lainnya.
	Switch	Alat yang digunakan untuk menyambungkan jaringan dengan komputer.

Kelompok Aset	Aset Kritis	Penjelasan
	Server	Digunakan sebagai penyimpanan data.
	Kabel jaringan	Kabel yang digunakan untuk menyambungkan jaringan dengan PC/Server/Router/Switch.
	CCTV	Digunakan untuk merekam kondisi.
Software	*Operating System* (Windows)	Sistem operasi yang digunakan pada PC yang digunakan dalam penjalanan proses bisnis.
	Aplikasi (Ms. Office, Corel Draw)	*Software* aplikasi pendukung yang digunakan dalam penjalanan proses bisnis
	Antivirus (Smadav)	*Software* yang menjaga PC dari serangan virus, *spyware* maupun *malware*.
Jaringan internet	Jaringan internet	Penggunaan internet dikarenakan sebagian proses bisnis harus dilakukan dengan bantuan internet.
User/People	Admin	SDM yang menjalankan proses bisnis
Data	Data Mahasiswa	Berisikan data terkait mahasiswa Politeknik Kesehatan Kemenkes Semarang.
	Data Alumni	Berisikan data terkait mahasiswa yang telah selesai melakukan studinya di Politeknik Kesehatan Kemenkes Semarang.
	Data Pembayaran	Berisikan data terkait detail pembayaran yang dilakukan oleh mahasiswa
	Data Pengajuan Proposal *Online*	Berisikan data terkait dosen atau mahasiswa yang mengajukan proposal secara *online.*

3.2 Kebutuhan Keamanan

Setelah mendapatkan info atas aset kritis perusahaan, kemudian dilakukan penentuan berdasarkan aspek keamanan informasinya terhadap aspek CIA yang terdiri atas:

1. *Confidentiality* (Kerahasiaan)
   Merupakan aspek penjamin kerahasiaan data atau informasi dan memastikan bahwa informasi hanya bisa diakses oleh orang yang memiliki wewenang dan menjamin kerahasiaan informasi.
2. *Integrity* (Integritas)
   Merupakan aspek penjamin tidak adanya perubahan data tanpa ijin pihak berwenang (*authorized*), menjaga keakuratan, dan keutuhan info.
3. *Availability* (Ketersediaan)
   Merupakan aspek penjamin data akan tersedia saat dibutuhkan oleh user yang memiliki wewenang (berhak) menggunakan informasi dan perangkat terkait.

3.3 Ancaman Aset Kritis

Ancaman aset kritis ditentukan berdasarkan kemungkinan terjadi atas aset, ancaman ditentukan dengan melakukan *brainstorming* dengan Ketua Divisi TI.

3.4 Penerapan Keamanan

1. Pihak terkait divisi TI harus paham tentang penggunaan dasar atas aset yang dimiliki. Kebijakan ini diterapkan agar penggunaan aset sesai dengan yang seharusnya.

2. Pembatasan hak akses. Tiap admin memiliki wewenangnya sendiri, dengan password dan username yang berbeda untuk tiap progdi sehingga modifikasi data hanya dapat dilakukan oleh admin progdi terkait.
3. *Back-up* data. *Back-up* data memang sudah dilakukan oleh pihak ketiga, akan tetapi pihak Politeknik Kesehatan Kemenkes Semarang tetap melakukan *back-up* secara mandiri.

3.5 Kelemahan Divisi TI

1. Kekurangan Sumber Daya Manusia (SDM).
2. Belum memiliki standar keamanan.
3. *Bandwidth* kurang.
4. Jumlah CCTV kurang, sehingga tidak bisa mengawasi ruang divisi TI secara jelas
5. Penggunaan *software* masih bajakan.

3.6 Daftar Komponen Kunci

Komponen kunci merupakan unsur kunci yang dalam penerapannya mendukung proses bisnis utama.

Tabel 3.2 Daftar Komponen Kunci

Kelompok	*Key Component*	Penjelasan
Hardware	PC	Digunakan untuk menunjang proses bisnis utama.
	Server	Digunakan sebagai penyimpanan data.
Software	*Operating System*	Sistem operasi yang digunakan pada PC yang digunakan dalam penjalanan proses bisnis oleh tiap admin.
	Aplikasi	Aplikasi yang digunakan para admin dalam mengelola data dalam proses bisnis utama.
Jaringan internet	Jaringan internet	Penggunaan internet dikarenakan sebagian proses bisnis harus dilakukan dengan bantuan internet.
User/People	Admin	Merupakan orang-orang yang memiliki wewenang dalam melakukan proses bisnis divisi IT pada Politeknik Kesehatan Kemenkes Semarang.
Data	*Database*	Sebagai tempat penyimpanan data yang berkaitan dengan proses bisnis yang dijalankan oleh divisi IT.

3.7 Evaluasi Komponen Kunci

Komponen Kunci dievaluasi untuk menentukan kemungkinan kelemahan dan penjelasannya.

3.8 Analisis Risiko

Pada tahap ini risiko akan di evaluasi agar dapat menentukan tingkatan dampak maupun penyebab dan dampak ancaman risiko aset kritis beserta pemilik risiko.

3.9 Nilai Risiko

Menentukan masalah dengan nilai risiko paling serius (tinggi) dilakukan dengan cara mencari tau bagaimana kesalahan akan terjadi dan bagaimana kesalahan akan memberikan dampak pada organisasi. Setelah sebelumnya risiko telah dianalisa, penilaian dilakukan untuk mengetahui seberapa serius tingkatannya dengan memanfaatkan metode FMEA.

3.10 Ranking Risiko

Perankingan risiko dilakukan dengan mengurutkan jumlah RPN tiap aset dari tertinggi hingga terendah.

3.11 Mitigasi Risiko

Mitigasi risiko ditentukan tindakan yang disarankan beserta jenisnya. Empat jenis mitigasi risiko yaitu *Tolerate, Treat, Transfer,* dan *Terminate*[7].

1. *Tolerate* : Ditujukan kepada risiko yang masih dapat diterima, baik itu karena dampak dari risiko maupun kemungkinan untuk terjadinya risiko yang cukup kecil bagi organisasi.
2. *Treat* : Ditujukan kepada risiko yang kemungkinan memiliki dampak yang tidak terlalu besar bagi organisasi namun memiliki tingkat kemungkinan untuk terjadi yang tinggi.
3. *Transfer* : Ditujukan kepada risiko yang memiliki dampak cukup besar bagi organisasi namun memiliki tingkat kemungkinan untuk terjadi cukup rendah.
4. *Terminate* : Ditujukan kepada risiko yang memiliki dampak besar bagi perusahaan dan tingkat kemungkinan untuk terjadi tinggi.

3.12 Penerapan Kontrol ISO 27002:2013

ISO 27002:2013 membantu dalam pembentukan pedoman pelaksanaan kontrol keamanan informasi atas masing-masing penyebab risiko tiap aset teknologi informasi pada Politeknik Kesehatan Kemenkes Semarang.

Tabel 3.3 Penerapan Kontrol ISO 27002:2013[6]

ID Risk	***Cause***	***Objective Control***
SR04	Aplikasi tidak original sehingga kesalahan program dalam pemakaian cukup tinggi.	A.12.5.1 *Installation of software on operational systems* Prosedur yang jelas harus diimplementasikan untuk mengontrol proses installasi *software* pada sistem operasi.
HR02	Terputusnya aliran listrik ketika penggunaan PC sedang dilakukan.	A.11.2.2 *Supporting utilities* Perangkat harus dilindungi dari kegagalan penyedia tenaga listrik, misal dengan menggunakan penyedia tenaga listrik cadangan UPS agar memberikan waktu untuk menyimpan pekerjaan maupun menghidupkan genset.
SR01	Pemakaian media penyimpanan *eksternal* yang sembarangan sehingga rentan masuknya virus.	A.7.2.1 *Management responsibilities* Manajemen tanggung jawab bagi pegawai dalam mengelola keamanan informasi sesuai dengan syarat ketentuan dan prosedur dari organisasi, sehingga diharapkan pegawai tidak sembarangan dalam menggunakan media penyimpanan *eksternal.* A.8.3.1 *Management of removable media* Prosedur yang jelas harus diterapkan dalam pengelolaan media penyimpanan eksternal. A.11.2.8 *Unattended user equipment* Pengguna harus yakin bahwa penggunaan media *eksternal* yang belum terdaftar memiliki cukup perlindungan. A12.2.1 *Controls against malware* Kontrol deteksi, pencegahan dan pemulihan akibat *malware* harus diterapkan, dikombinasikan dengan sikap

ID Risk	*Cause*	*Objective Control*
		hati-hati dari *user*.
JI03	Jaringan *down* dari pusat penyedia layanan.	A.13.1.2 *Security of networks services* Mekanisme keamanan, level servis dan syarat manajemen dari semua servis jaringan harus diidentifikasikan dan dimasukkan dalam persetujuan kontrak servis jaringan, baik itu untuk internal maupun jaringan yang disediakan oleh pihak lain.
HR11	Virus masuk dari media penyimpanan *eksternal* maupun didapat ketika berselancar di internet.	A.7.2.1 *Management responsibilities* Manajemen tanggung jawab bagi pegawai dalam mengelola keamanan informasi sesuai dengan syarat ketentuan dan prosedur dari organisasi, sehingga diharapkan pegawai tidak sembarangan dalam menggunakan media penyimpanan *eksternal*. A.8.3.1 *Management of removable media* Prosedur yang jelas harus diterapkan dalam pengelolaan media penyimpanan *eksternal.* A.11.2.8 *Unattended user equipment* Pengguna harus yakin bahwa penggunaan media *eksternal* yang belum terdaftar memiliki cukup perlindungan. A12.2.1 *Controls against malware* Kontrol deteksi, pencegahan dan pemulihan akibat malware harus diterapkan, dikombinasikan dengan sikap hati-hati dari *user*.
SR02	Antivirus gagal melakukan *scan* virus/*malware* yang ada.	A12.2.1 *Controls against malware* Kontrol deteksi, pencegahan dan pemulihan akibat malware harus diterapkan, dikombinasikan dengan sikap hati-hati dari *user*. A.12.5.1 *Installation of software on operational systems* Prosedur yang jelas harus diimplementasikan untuk mengontrol proses installasi *software* pada sistem operasi.
JI01	Kurangnya pengamanan atas jaringan yang dimiliki sehingga *hacking* memungkinkan untuk terjadi	A.13.1.1 *Network Controls* Kontrol jaringan harus dikelola dan dikontrol untuk melindungi aset yang ada dan berhubungan dengan jaringan. A.13.1.2 *Security of network services* Mekanisme keamanan, level servis dan syarat manajemen dari semua servis jaringan harus diidentifikasikan dan dimasukkan dalam persetujuan kontrak servis jaringan, baik itu untuk internal maupun jaringan yang disediakan oleh pihak lain.
DA03	Data rusak karena eror saat proses menyimpan maupun karena serangan virus.	A.12.2.1 *Controls against malware* Kontrol deteksi, pencegahan dan pemulihan akibat *malware* harus diterapkan, dikombinasikan dengan sikap hati-hati dari user. A.12.5.1 *Installation of software on operational systems* Prosedur yang jelas harus diimplementasikan untuk mengontrol proses installasi software pada sistem operasi.
HR09	Akibat terkena bencana alam	A.11.1.4 *Protecting against external and environmental threats* Perlindungan dari bencana alam, serangan berbahaya atau kecelakaan harus di rancang dan diterapkan.

ID Risk	*Cause*	*Objective Control*
HR05	Maintenance PC tidak teratur hingga perawatan bagi bagian PC yang membutuhkan terabaikan.	A.11.2.4 *Equipment maintenance* Perangkat harus mendapatkan *maintenance* yang teratur dan benar untuk memastikan perangkat tersebut tetap tersedia kapanpun ketika dibutuhkan dan integritas yang selalu terjaga.
HR07	PC digunakan oleh *user* secara berlebihan.	A.12.1.1 *Documented operating procedures* Prosedur operasi harus memiliki dokumentasi dan harus tersedia ketika user yang berhak membutuhkannya.
HR33	Kabel terinjak/sengaja dirusak oleh manusia.	A.9.4.1 *Information access retriction* Akses kepada sistem atau aplikasi dibatasi dengan kebijakan akses kontrol A.11.1.1 *Physical security perimeter* Perimeter keamanan harus dimiliki dan digunakan untuk melindungi area aset yang didalam nya terdapat informasi kritis maupun dan fasilitas pengolahan informasi. A.11.1.2 *Physical entry controls* Area aman harus dilindungi oleh kontrol masuk yang sesuai untuk memastikan bahwa hanya orang-orang yang memiliki ijin yang dapat mengakses. A.11.2.3 *Cable security* Kabel harus dijaga dari gangguan, pemotongan atau perusakan.
HR34	Kabel terputus akibat digigit oleh binatang.	A.11.2.3 *Cable security* Kabel harus dijaga dari gangguan, pemotongan atau perusakan.
SR05	*Maintenance* kurang, sehingga kerusakan awal tidak terdeteksi.	A.11.2.4 *Equipment maintenance* Perangkat harus mendapatkan *maintenance* yang teratur dan benar untuk memastikan perangkat tersebut tetap tersedia kapanpun ketika dibutuhkan dan integritas yang selalu terjaga.
HR03	Akibat konsleting antar komponen	A.11.2.4 *Equipment maintenance* Perangkat harus mendapatkan *maintenance* yang teratur dan benar untuk memastikan perangkat tersebut tetap tersedia kapanpun ketika dibutuhkan dan integritas yang selalu terjaga.
HR04	PC tidak disimpan di tempat yang aman, sehingga PC jatuh dari ketinggian dan rusak.	A.11.1.5 *Procedures for working in secure areas* Prosedur untuk bekerja di area yang aman harus dirancang dan diterapkan.
HR06	Pemakaian PC oleh *user* tidak sesuai dengan prosedur yang seharusnya	A.12.1.1 *Documented operating procedures* Prosedur operasi harus memiliki dokumentasi dan harus tersedia ketika user yang berhak membutuhkannya.
UP01	*User* kurang memiliki kemampuan dalam menggunakan maupun mengatasi masalah atas aset yang mendukung berjalannya aset kritis.	A.7.2.2 *Information seurity awareness, education, and training* Semua pegawai organisasi, kontraktor, maupun yang memiliki hubungan bisnis harus menerima pendidikan yang pantas dan pelatihan maupun pembaharuan informasi kebijakan organisasi yang sesuai dengan pekerjaan masing-masing.

4. KESIMPULAN

1. Berdasarkan proses identifikasi risiko aset teknologi informasi pada Politeknik Kesehatan Kemenkes Semarang, diperoleh 50 risiko dimana 10 risiko memiliki ranking *very high,* 8 risiko dengan ranking *high*, 18 risiko dengan ranking *moderate*, 13 risiko dengan ranking *low* dan 1 risiko dengan ranking *very low*.
2. Dengan menggunakan metode FMEA didapatkan risiko dengan level tertinggi hingga terendah, sehingga Politeknik Kesehatan Kemenkes Semarang dapat mengambil tindakan prioritas kepada risiko dengan ranking *very high* dan *high*. Hal ini dilakukan karena risiko dengan level *very high* dan *high* memberikan dampak yang besar kepada organisasi sehingga risiko dapat diminimalisir atau bahkan dicegah sebelum terjadi.
3. Berdasarkan penilaian yang telah dilakukan dengan menggunakan metode FMEA, tindakan kontrol risiko kepada ranking risiko *very high* dan *high* telah diberikan dengan mengacu pada ISO 27002:2013 yang memiliki fokus standarisasi Sistem Manajemen Keamanan Informasi (SMKI) agar risiko dapat diminimalisir atau bahkan dihilangkan

5. SARAN

Menerapkan standar ISO yang berbeda untuk mendapatkan hasil yang lebih bervariasi dan sesuai kebutuhan pada Politeknik Kesehatan Kemenkes Semarang. Misal ISO 14001 yang merupakan standar dengan isi persyaratan sistem manajemen limgkungan, dimana perusahaan harus melakukan identifikasi atas aspek dan dampak lingkungan yang merupakan akibat dari kegiatan maupun operasi organisasi terhadap aspek lingkungan.

DAFTAR PUSTAKA

[1] C. Alberts and A. Dorofee, “Introduction to the OCTAVE Approach,” *... , PA, Carnegie Mellon ...*, no. August, pp. 1–37, 2003.

[2] C. S. Carlson, “Understanding and Applying the Fundamentals of FMEAs,” *2014 Annu. Reliab. Maintainab. Symp.*, p. 12, 2014.