Risk Management Aset Teknologi Informasi Menggunakan *Framework* OCTAVE (*Operationally Critical Threat, Asset And Vulnerability Evaluation)* Dan FMEA (*Failure Mode And Effect Analysis) Di Universitas Muhammadiyah Yogyakarta*

Risk Management Aset Teknologi Informasi Menggunakan *Framework* OCTAVE (*Operationally Critical Threat, Asset And Vulnerability Evaluation)* Dan FMEA (*Failure Mode And Effect Analysis*) Di Universitas Muhammadiyah Yogyakarta

ADIKA MANDALA ARFIANDA YUHAZ, CHAYADI OKTOMY NOTO S, DWIJOKO PURBOHADI

ABSTRACT

Penerapan teknologi pada Universitas Muhammadiyah Yogyakarta dapat membantu proses dari pengolahan data dan informasi yang prosesnya berkaitan langsung dengan mahasiswa, staff ataupun dosen pada institusi pendidikan. Permasalahan yang pernah dialami pada Universitas Muhammadiyah Yogyakarta seperti adanya percobaan masuk ke sistem dari orang yang tidak bertanggung jawab. Kejadian tersebut berakibat kegiatan operasional terganggu untuk sesaat. Tujuan dari penelitian ini adalah untuk mengetahui apa saja aset teknologi informasi yang ada pada Universitas Muhammadiyah Yogyakarta, menganalisis dan mengevaluasi untuk memperkecil risiko yang terjadi pada setiap aset teknologi informasi serta dapat mengetahui hasil penilaian atas mitigasi risiko aset teknologi informasi. Metode penelitian yang digunakan yaitu OCTAVE untuk mengolah risiko aset teknologi informasi dan FMEA untuk melakukan penilaian ke masing-masing risiko, yang selanjutnya diberikan ranking berdasarkan prioritasnya.
Keywords: FMEA, OCTAVE, Teknologi Informasi, RPN

1. PENDAHULUAN

Dalam perkembangan teknologi informasi saat ini keamanan aset informasi merupakan sebuah aspek penting di sebuah organisasi yang penting untuk dilindungi dari risiko keamanannya baik dari pihal luar dan dalam dari organisasi. Manajemen risiko meliputi tiga proses yaitu: risiko penilaian, mitigasi risiko dan evaluasi dan penilaian [1]

Kegiatan ini dibutuhkan untuk mendukung misi organisasi dan melindungi aset dari organisasi tersebut. Pada IT Risk Management, erat kaitannya dengan bagaimana implementasi security pada suatu organisasi sehingga diperlukan pemahaman tentang proses bisnis organisasi dan kemungkinan resiko yang berdampak pada proses bisnis tersebut. Risk Management akan sangat membantu manajemen organisasi untuk menyeimbangkan antara dampak dari *risk* yang dibutuhkan untuk meminimalisir resiko tersebut [2].

Tujuan dari penelitian ini adalah untuk mengetahui aset teknologi informasi yang ada pada Universitas Muhammadiyah Yogyakarta, menganalisis dan mengevaluasi untuk memperkecil risiko yang terjadi pada setiap aset teknologi informasi, serta dapat mengetahui hasil penilaian atas mitigasi risiko aset teknologi informasi.

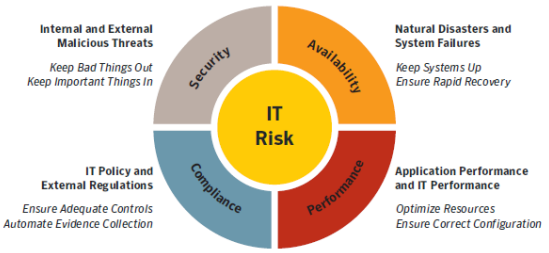
Untuk mengetahui ancaman dan risiko keamanan informasi dibutuhkan kemampuan dalam pengelolaan risiko keamanan informasi dari pengguna teknologi yang digunakan. Maka dibutuhkan suatu pendekatan ilmu manajemen keamanan sistem informasi. Untuk mengetahui tingkat risiko yang terjadi pada Universitas Muhammadiyah Yogyakarta, maka diperlukan suatu langkah penilaian terhadap risiko yang mungkin akan muncul dan dapat mengakibatkan keberlangsungan bisnis dan menimbulkan kerugian pada Universitas Muhammadiyah Yogyakarta. Maka dari itu untuk mengetahui risiko dari penggunaan TI, diperlukan sebuah metode atau kerangka kerja untuk membantu proses penilaian risiko.Beberapa metode yang dapat digunakan untuk penilaian risiko seperti metode OCTAVE (*Operationally Critical Threat, Asset And Vulnerability Evaluation*) Dan FMEA (*Failure Mode And Effect Analysis*). Metode

OCTAVE merupakan teknik strategi dan perencanaan untuk keamanan atas risiko [3]. Dan pemakaian FMEA untuk menilai risiko yang mungkin akan terjadi kedepan dengan mempersiapkan proses, desain maupun kendala dari risiko [4]. Dan selanjutnya menggunakan metode RPN yang merupakan metode pemberian peringkat dari setiap risiko kegagalan yang berada pada sistem atau organisasi berdasarkan penghitungan dari tiga elemen yaitu, severity (dampak), occurrence (frekuensi), detection (deteksi). RPN akan mempengaruhi pilihan yang diambil untuk mengatasi kegagalan sebuah sistem.[5]
Proses penilaian menggunakan metode FMEA dan RPN. Risiko dengan ranking *high* memberi pengaruh yang begitu besar pada Universitas Muhammadiyah Yogyakarta maka dari itu risiko bisa di perkecil ataupun bisa dilakukan pencegahan sebelum terjadi masalah atau kerusakan pada aset yang dimiliki.

2. LANDASAN TEORI

2.1 Information Technology *Risk Management*

Information technology risk management adalah peluang atau kemungkinan dari suatu bahaya, kehilangan atau konsekuensi buruk lainnya. Risiko merupakan potensi dari kerusakan pada *organization value,* sering kali dari proses manajemen dan kejadian yang tidak memadai dan dapat dianggap sebagai komponen dari sistem menejemen risiko. Risk management yaitu tentang ketidakpastian dari peristiwa di masa yang akan datang. [6] Berdasarkan kerangka kerja risiko teknologi informasi ini tidak hanya mencakup dampak negatif seperti risiko yang mungkin dihadapi di organisasi yang berhubungan dengan keuangan atau transaksi. Risiko Bisnis dari Komponen Operasional merupakan hasil daripada transaksi termasuk risiko dari internal seperti kualitas produk, organisasi, dan kinerja pabrik, sedangkan dari eksternal terkait dengan bencana alam atau ada perubahan dalam peraturan pemerintahan.



Gambar 1 Klasifikasi Information Technology Management

Kerangka kerja pada Gambar 2.1 mengklasifikasikan *Information Technology Risk* sebagai berikut: [7]

1. *Security Risk* – Informasi itu akan diubah, diakses atau digunakan oleh pihak yang tidak berwenang.
2. *Availability Risk* – Informasi atau aplikasi tidak dapat diakses karena kegagalan sistem atau bencana alam, ancaman ini termasuk sebagai periode yang memakan waktu lama untuk pemulihannya.
3. *Performance Risk* – Yaitu kinerja yang kurang baik dari sistem, aplikasi, personal atau teknologi informasi dengan keseluruhan akan mengurangi produktivitas atau nilai bisnis.
4. *Compliance Risk* – Yaitu penanganan atau pemrosesan informasi yang gagal memenuhi persyaratan peraturan dari suatu kebijakan teknologi informasi dan bisnis.

Dari keempat kategori ini sudah dapat mengklasifikasikan semua elemen *Information technology risk management.*
Manfaat manajemen risiko juga dapat diidentifikasi dalam kaitannya dengan tiga kali skala kegiatan dalam organisasi.[8] Output dari kegiatan manajemen risiko dapat menguntungkan organisasi dalam tiga skala waktu dan memastikan bahwa organisasi mencapai:

1. Strategi yang efektif
2. Proses dan proyek yang efektif
3. Operasi yang efisien

Untuk mencapai kontribusi manajemen risiko yang berhasil, manfaat yang diharapkan dari setiap inisiatif manajemen risiko harus diidentifikasi. Jika hasil itu belum teridentifikasi, maka tidak akan ada sarana untuk mengevaluasi apakah manajemen risiko telah berhasil. Oleh karena itu, manajemen risiko yang baik harus memiliki serangkaian hasil / manfaat yang jelas. Perhatian yang tepat harus diberikan kepada setiap tahap proses manajemen risiko, serta rincian desain, implementasi dan pemantauan kerangka kerja

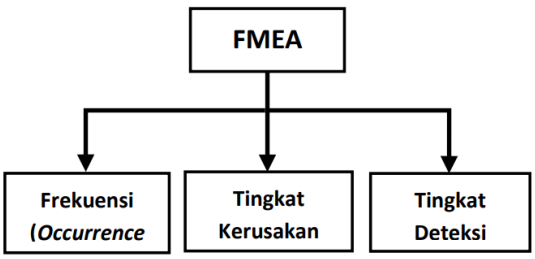
yang mendukung kegiatan manajemen risiko ini.

2.2 Metode FMEA (Failure Mode and Effect Analysis)

FMEA (*Failure Mode and Effect Analysis*) adalah cara yang terstruktur untuk mengidentifkasi dan mengatasi masalah potensial, atau kegagalan dan efek yang dihasilkan pada sistem atau proses sebelum suatu peristiwa buruk terjadi, FMEA akan mengidentifikasi dan akan menghilangkan proses kegagalan untuk mencegah suatu peristiwa yang tidak diinginkan [4]. Menilai suatu risiko dengan proses kegagalan yang teridentifikasi efek, penyebabnya dan memperioritaskan masalah yang ada agar dapat dilakukan tindakan korektif. FMEA harus menjadi panduan *development* untuk menyelesaikan tindakan yang akan mengurangi risiko yang terkait dengan sistem, subsistem, dan komponen atau proses manufaktur / perakitan ke tingkat yang dapat diterima. Tujuan dari FMEA adalah membantu untuk merancang kegagalan yang terindikasi dari sistem dengan biaya terendah dalam hal waktu dan uang. Berikut adalah proses dari FMEA [9]

2.2.1 Langkah-langkah Proses FMEA

Dalam penelitian ini FMEA dilakukan untuk melihat risiko-risiko yang mungkin terjadi pada operasi perawatan dan kegiatan operasional perusahaan. Dalam hal ini ada tiga hal yang membantu menentukan dari gangguan antara lain:



Gambar 2 Skema Parameter FEMA

1. Dampak kegagalan (Severity)
2. Dalam menentukan tingkat kerusakan (severity) ini dapat ditentukan seberapa serius kerusakan yang dihasilkan dengan terjadinya kegagalan proses dalam hal operasi perawatan dan kegiatan operasional organisasi. [10]
3. Frekuensi (Occurrence)
4. Dalam menentukan occurrence ini dapat ditentukan seberapa banyak gangguan yang dapat menyababkan sebuah kegagalan pada operasi perawatan dan kegiatan operasional organisasi.
5. Tingkat Deteksi (Detection)
6. Detection menunjukan seberapa besar kemungkinan kegagalan itu akan terdeteksi. Semakin tinggi nilai pada detection maka semakin besar kemungkinan kegagalan tidak akan terdeteksi. dimana nilai 1 mengindikasikan tidak adanya kesalahan, nilai 10 mengindikasikan tingkat kesalahan sangat sulit di deteksi. [11]

2.3 Risk Priority Number (RPN)

Merupakan metode yang memberi peringkat dari setiap risiko kegagalan yang berada pada sistem atau organisasi berdasarkan penghitungan dari tiga elemen yaitu, severity (dampak), *occurrence* (frekuensi), *detection* (deteksi). RPN akan mempengaruhi pilihan yang diambil untuk mengatasi kegagalan sebuah sistem. Hasil RPN akan menunjukan area yang paling bermasalah, dan RPN dengan peringkat tertinggi harus mendapatkan prioritas tertinggi dalam pengambilan tindakan untuk menyelesaikan permasalahan. Tujuan dari pengambilan tindakan yaitu, menghilangkan potensi kegagalan, mengurangi dampak dari kegagalan, mengurangi frekuensi kegagalan, dan memudahkan deteksi kegagalan. [9]

$$\boldsymbol{RPN = S * O * D \ (or \ RPN = S \ x \ O \ x \ D)}$$

1. RPN = (Risk Priority Number) yaitu metode pemberian peringkat dari setiap risiko kegagalan yang ada
2. S = Severity (Dampak) yaitu dampak yang ditimbulkan dari setiap aset risiko yang ada
3. O = Occurrence (Frekuensi Kegagalan) yaitu seberapa sering kegagalan itu terjadi
4. D = Detection (Deteksi Kegagalan) yaitu seberapa besar kemungkinan kemungkinan kegagalan itu akan terjadi

2.2 Metode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*) merupakan kerangka kerja untuk mengidentifikasi dan mengelola risiko keamanan informasi [3] . Kerangka kerja ini berfokus pada permasalahan strategi dan praktik keamanan yang terkait, dengan begitu organisasi dapat merancang dan menerapkan strategi perlindungan untuk

mengurangi risiko keseluruhan aset informasinya. OCTAVE lebih pada penerapan praktik keamanan ditujukan pada internal organisasi dan strategi untuk mengantisipasi keamanan di masa yang akan datang dan diselaraskan dengan kepentingan organisasi.

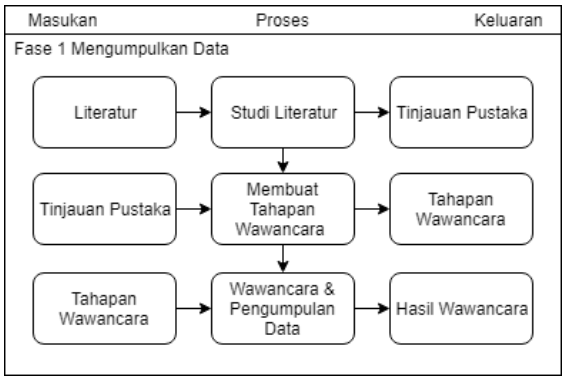
1. Fase 0: Persiapan *(Preparation)*
2. Hal penting yang harus dipersiapkan sebelum melaksanakan kerangka kerja OCTAVE ada tiga cara yaitu menyusun jadwal, membentuk tim analis, mempersiapkan peralatan.
3. Fase 1: Membangun Aset Berbasis Profil Ancaman
4. Tim analisis menentukan apa yang penting bagi organisasi dan apa yang saat ini sedang diterapkan dalam melindungi aset. Setelah itu dipilih mana yang paling penting bagi organisasi yaitu aset kritis dan dideskripsikan kebutuhan keamanan ancaman dan profil ancaman pada masing – masing aset kritis. [3]
5. Fase 2: Mengidentifikasi Kerentanan Infrastruktur
6. Pada proses OCTAVE yang kedua, mengidentifikasi kerentanan infrastruktur menjelaskan tentang aktifiktas untuk mendapatkan pengetahuan berupa aset, ancaman dan strategi pengamanan dari orang yang berada pada bidang terkait. Tujuan lain sebagai tindakan evaluasi atas informasi infrastruktur. [3]
7. Fase 3: Mengembangkan rencana dan strategi keamanan
8. 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 analisis informasi yang telah dikumpulkan.

3. METODE PENELITIAN

Metode yang akan digunakan pada penelitian ini menggunakan dua metode yaitu:Metode OCTAVE berguna untuk mengelola hasil wawancara dari narasumber.

Metode FMEA berguna untuk memberikan hasil berupa nilai pada tiap aset teknologi informasi yang sebelumnya sudah didefiniskan pada metode OCTAVE.

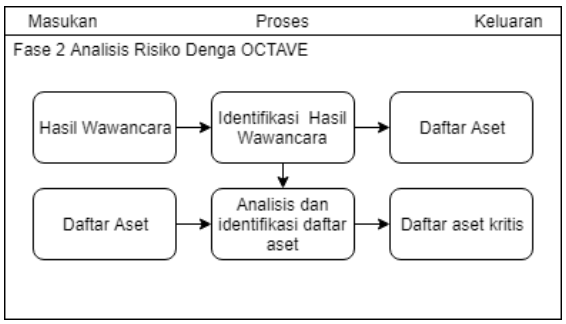
3.1.1. Fase Pertama – Mengumpulkan Data



Gambar 4 Mengumpulkan Data

Pada fase pertama peneliti melakukan studi literatur berupa pembuatan tahapan wawancara, selanjutnya peneliti akan meninjau kembali hasil studi literatur yang nantinya akan dilakukan pembuatan tahapan wawancara. Wawancara dilakukan ke Universitas Muhammadiyah Yogyakarta pada bagian Divisi Sistem Informasi, wawancara terfokus kepada ketua maupun kepala urusan bidang sistem informasi. Setelahnya hasil wawancara akan dikumpulkan agar bisa dilakukan analisis. Analisis selanjutnya akan menggunakan metode OCTAVE.

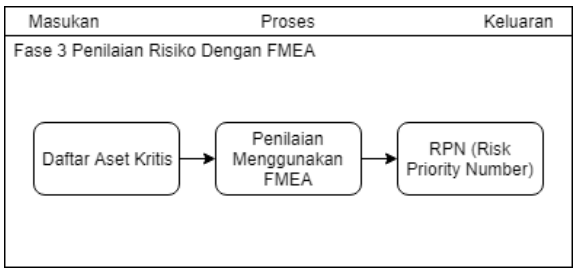
3.1.2. Fase Kedua – Analisis Risiko Dengan OCTAVE



Gambar 5 Analisis Risiko Dengan OCTAVE

Pada fase kedua peneliti akan mengelola data hasil wawancara yang melalui proses analisis dan identifikasi yang hasil akhirnya berupa daftar aset, ini merupakan hasil kerangka kerja dari OCTAVE. Daftar aset keamanan yang sudah dilakukan sebelumnya, dan selanjutnya dilakukan pengurutan daftar aset penting dengan penilaian RPN (*Risk Number Priority*), ini merupakan hasil kerangka kerja FMEA. Hasil dokumentasi didapat dari kelemahan sistem yang dimiliki oleh Universitas Muhammadiyah Yogyakarta.

3.1.3. Fase Ketiga – Penilaian Risiko Dengan FMEA



Gambar 6 Analisis Risiko Dengan FMEA

Pada fase ketiga daftar aset kritis akan dilakukan penilaian menggunakan FMEA untuk dianalisa dan diurutkan berdasarkan tingkat risiko tertinggi yang memiliki risiko paling besar jika terjadi kegagalan proses bisnis. Selanjutnya berdasarkan tiga elemen yang ada pada metode RPN yaitu, *severity*, *occurrence*, dan *detection* akan diberi pemeringkatan dari setiap risiko yang berada pada sistem atau organisasi.

3.1.4. Fase Keempat – Membuat Laporan Hasil Penelitian

Pada fase keempat hasil yang telah didapatkan berupa daftar dari aset kritis yang sudah dicari. Hasil yang sudah didokumentasikan akan diserahkan ke Divisi Sistem Informasi di Universitas Muhammadiyah Yogyakarta.

3.2. Sumber Data

Data bersumber dari hasi wawancara dan dari jurnal atau perantara buku. Data akan dijelaskan dibagi menjadi 2 yaitu :

3.2.1. Data Primer

Adalah data yang diperoleh langsung dari sumber asli atau pihak pertama. Dalam penelitian ini data primer didapat dari wawancara kepada karyawan dan observasi langsung ke Divisi Sistem Informasi yang terkait.

3.2.2. 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.

4. HASIL PEMBAHASAN

4.1 Proses Pengumpulan Data Aset

Pada proses pengumpulan data aset, peneliti melakukan berbagai metode wawancara ke narasumber. Wawancara berupa rekaman dengan narasumber dan berupa pencatatan dari pemaparan yang dijelaskan oleh narasumber. Dalam proses pengumpulan data aset, peneliti melakukan studi literatur terkait kerangka kerja yang digunakan yaitu OCTAVE dan FMEA sebagai landasan peneliti untuk membuat daftar pertanyaan untuk wawancara.

3.2 Mendata Aset Kritis

Dari hasil wawancara yang sudah dilakukan untuk mendata dan mencari informasi dari Universitas Muhammadiyah Yogyakarta maka diperoleh data aset kritis teknologi informasi yang dijelaskan pada Tabel 1 berikut :

Kategori Aset	Aset Kritis
Hardware	Server
	Switch
	Accesspoint
	Kabel LAN
	PC
	Core Switch
	PC Storage Hitachi
	Router
	WLC (Wireless LAN Controller)

	Firewall
Software	Web Kartu Rencana Studi Daring (KRS Daring).
	Web Repository
	Web E-Learning
	DHCP Server
	SIM Surat
	SIM Anggaran
	SIM Arsip
	SIM Aset
	SIM Kepegawaian
	SIM MoU
	Web Portal Institusi
	Web Portal Fakultas
	Web Portal Program Studi
	ASP .NET dan IIS
Data	Data Web Kartu Rencana Studi Daring (KRS Daring).

Tabel 1 Tabel Aset Kritis

3.3. Identifikasi Kondisi Aset Saat Ini

Pada proses identifikasi kondisi aset saat ini hasil dari proses pengumpulan data aset yang sudah didapat, maka data tersebut akan diolah dan di identifikasi berdasarkan daftar aset. Selanjutnya akan dianalisis menggunakan kerangka kerja OCTAVE hasilnya berupa nilai *severity*, *occurrence*, dan *detection*. Dan selanjutnya digunakan untuk menghitung RPN (*Risk Priority Number*). Tabel 4.2 menampilkan daftar aset yang ada sekarang pada Universitas Muhammadiyah Yogyakarta.

NO	Aset	Problem
1	Web Kartu Rencana Studi Online.	Percobaan manipulasi dan kebocoran data.
		Mahasiswa masih menggunakan password bawaan.
		Masih ada data mahasiswa yang tidak valid.
2	Web Repository	Paling banyak terkena serangan dari eksternal.
		Kebutuhan penyimpanan semakin meningkat.
		Web belum secure dan tidak ada SSL Certificate
3	Core Switch	Percobaan masuk kedalam sistem.
4	PC Storage Hitachi	Perlu pembaharuan storage secara berkala.
5	Web E-Learning	Kebutuhan penyimpanan semakin meningkat.
		Web belum secure dan tidak ada SSL Certificate
6	Switch	Belum pernah dilakukan evaluasi pada perangkat tersebut.
7	Router	Rusak apabila karena factor alam.

		Belum pernah dilakukan evaluasi pada perangkat tersebut.
8	SIM Surat	Kebocoran dan Manipulasi data.
9	DHCP Server	Tidak ada.
10	Wireless LAN Controller	Perangkat mengalami kerusakan fisik.
		Kesalahan konfigurasi pada perangkat.
11	SIM Anggaran	Kebocoran dan Manipulasi data.
12	SIM Arsip	Kebocoran dan Manipulasi data.
13	SIM Aset	Kebocoran dan Manipulasi data
14	SIM Kepegawaian	Kebocoran dan Manipulasi data.
15	SIM MoU	Kebocoran dan Manipulasi data.
16	Web Portal Institusi	Web belum secure dan Tidak ada SSL Certificate.
17	Web Portal Fakultas	Web belum secure dan Tidak ada SSL Certificate.
18	Web Portal Prodi	Web belum secure dan Tidak ada SSL Certificate.
19	Access Point	Belum pernah dilakukan evaluasi pada perangkat tersebut.
20	Firewall	Tidak ada
21	ASP .NET dan IIS	Tidak ada

Tabel 2 Analisis Risiko Dengan FMEA

3.4. Mengidentifikasi Ancaman Aset Kritis

Proses identifikasi suatu ancaman dilakukan pada masing-masing aset kritis teknologi informasi yang dimiliki Universitas Muhammadiyah Yogyakarta yang disertai dengan penyebab dari terjadinya ancaman tersebut.

3.5. Mengidentifikasi Kelemahan Universitas Muhammadiyah Yogyakarta

Dari hasil wawancara ditemukan beberapa kelemahan dalam mengamankan aset kritis teknologi informasi yang dimiliki Universitas Muhammadiyah Yogyakarta diantaranya adalah belum terealisasinya DRC (*Disaster Recovery Center*) dan belum terlaksananya evaluasi komponen infrastruktur kelemahan secara rutin.

3.6. Hasil Penilaian Aset Kritis

Pada bagian ini hasil penilaian aset kritis sudah diberi penilaian/peringkat dimana hasil di dapat dari perhitungan menggunakan metode RPN berdasar kan tiga elemen yaitu *severity*, *occurrence*, *detection* hasil tersebut dikali agar dapat ditemukan nilai RPN. Selanjutnya diberi kategori berdasarkan level yang sesuai dengan nilai RPN. Cara menentukan level *high*, *medium*, dan *low* yaitu 1 – 64 rating untuk *low*, 65 – 124 rating untuk *medium*, 125 > rating untuk *high*.

NO	Aset	Kelompok	Problem	*Severity* (Dampak)		*Occurrence* (Frekuensi)		*Detection* (Deteksi)		*RPN*	Level
				Rating	Cause	Rating	Cause	Rating	Cause		
1	Web Kartu Rencana Studi Daring (KRS Daring).	Data	Percobaan manipulasi dan kebocoran data.	10	Pengamanan data belum maksimal, sehingga memungkinkan terjadi penyalahgunaan data mahasiswa.	3	Baru saja terjadi dan ada kemungkinan akan terjadi lagi.	10	Belum diketahui sumber percobaan kebocoran data	300	*High*

		Software	Mahasiswa masih menggunakan kata sandi bawaan.	8	Human Error	5	Serangan sering terjadi hampir setiap hari	3	Deteksi bisa dimonitor melalui firewall	120	*Medium*
		Data	Masih ada data mahasiswa yang tidak valid.	5	Penyampaian informasi melalui nomor telepon, atau alamat bisa salah karena data tidak valid	1	Terjadi saat pengisian data mahasiswa di KRS	3	Bisa diketahui saat verifikasi data mahasiswa	15	*Low*
2	Web Repository	Software	Paling banyak terkena serangan dari eksternal.	9	Data skripsi dan artikel civitas diorganisasi bisa diakses dan dimanipulasi oleh orang yang tidak bertanggungjawab	8	Serangan sering terjadi hampir setiap hari	2	Deteksi bisa dimonitor melalui firewall	144	*High*
		Software	Kebutuhan penyimpanan semakin meningkat.	7	Jika *storage* penuh, maka web repository tidak bisa diakses	1	Belum terjadi	3	*Storage* bisa dimonitor secara *real-time*	21	*Low*
		Software	Web belum aman dan tidak ada SSL Certificate	8	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga memudahkan pencurian data	1	Belum terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
3	Core Switch	Hardware	Percobaan masuk ke dalam sistem.	9	Jaringan bisa saja menjadi kacau ketika terjadi kerusakan alat atau kesalahan konfigurasi	4	Belum pernah terjadi kegagalan sistem	4	Deteksi berdasarkan laporan	144	*High*
4	PC Storage Hitachi 4 unit.	Hardware	Perlu pembaharuan storage secara berkala.	9	Jika media penyimpanan penuh, maka semua data sulit diakses	5	Beberapa kali terjadi	2	Berdasarkan laporan kerusakan	90	*Medium*
5	Web E-Learning	Software	Kebutuhan penyimpanan semakin meningkat.	7	Jika *storage* penuh, maka web *e-learning* tidak bisa diakses	4	Beberapa kali terjadi	3	*Storage* bisa dimonitor secara *real-time*	84	*Medium*
		Software	Web belum aman dan tidak ada SSL Certificate	9	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga memudahkan pencurian data	1	Belum terjadi	3	Deteksi bisa dimonitor melalui *firewall*	24	*Low*
6	Kabel LAN	Hardware	Terjadi kerusakan karena sudah lama dan dikarenakan faktor alam	9	Internet akan mati didaerah kabel yang rusak	4	Frekuensi kerusakan berdasarkan laporan	2	Deteksi berdasarkan laporan	72	*Medium*
7	Switch	Hardware	Belum pernah dilakukan evaluasi pada perangkat tersebut.	6	Identifikasi permasalahan sistem menjadi lebih lama	5	Frekuensi kerusakan berdasarkan laporan	2	Deteksi berdasarkan laporan	60	*Low*
8	Router	Hardware	Rusak apabila karena faktor alam.	6	Router rusak	3	Frekuensi kerusakan berdasarkan laporan	2	Deteksi berdasarkan laporan	36	*Low*
		Hardware	Belum pernah dilakukan evaluasi pada	6	Identifikasi permasalahan sistem menjadi lebih lama	1	Frekuensi kerusakan berdasarkan laporan	2	Deteksi berdasarkan laporan	12	*Low*

			perangkat tersebut.								
9	SIM Surat	Software	Kebocoran dan Manipulasi data.	7	Tidak bisa diakses	2	Belum pernah terjadi kegagalan sistem	2	Berdasarkan laporan kerusakan	28	*Low*
10	DHCP Server	Software	Tidak ada.	7	Jika terjadi gangguan berdampak pada jaringan seluruh institusi mati	2	Belum pernah terjadi kegagalan sistem	2	Berdasarkan laporan kerusakan	28	*Low*
11	Wireless LAN Controller	Hardware	Perangkat mengalami kerusakan fisik.	6	Koneksi internet disuatu area tidak berjalan	1	Kegagalan system beberapa kali terjadi yang diketahui berdasarkan laporan dari stackholder terkait	3	Diketahui saat ada koneksi down di area tertentu	18	*Low*
		Hardware	Kesalahan konfigurasi pada perangkat.	6	Koneksi internet disuatu area tidak berjalan	1	Belum pernah terjadi kegagalan sistem	3	Diketahui saat ada koneksi down di area tertentu	18	*Low*
12	SIM Anggaran	Software	Kebocoran dan Manipulasi data.	8	Surat Pertanggungjawaban yang dimanipulasi menyebabkan terhambatnya proses bisnis suatu unit kerja dan menyebabkan terhambatnya proses pencairan dana untuk kegiatan selanjutnya pada unit kerja tersebut	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
13	SIM Arsip		Kebocoran dan Manipulasi data.	8	SK pengangkatan seseorang yang sifatnya rahasia, bisa disalahgunakan.	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
14	SIM Aset		Kebocoran dan Manipulasi data	8	Terjadi kesalahan dalam proses perhitungan audit data. Duplikasi data aset yang bisa menyebabkan pihak lain mengakusisi salah satu atau beberapa asset milik Universitas Muhammadiyah Yogyakarta	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
15	SIM Kepegawaian		Kebocoran dan Manipulasi data.	8	Penyalahgunaan Informasi bisa menyebabkan penipuan mengatasnamakan perorangan atau instansi	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
16	SIM MoU		Kebocoran dan Manipulasi data.	8	Kemungkinan terjadinya kebocoran data menyebabkan diketahuinya pihak mana saja yang sudah menjalin kerjasama dengan	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*

					Universitas Muhammadiyah Yogyakarta						
17	Web Portal Institusi		Web belum aman dan Tidak ada SSL Certificate.	8	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
18	Web Portal Fakultas		Web belum aman dan Tidak ada SSL Certificate.	8	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
19	Web Portal Program Studi		Web belum aman dan Tidak ada SSL Certificate.	8	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
20	Access Point		Belum pernah dilakukan evaluasi pada perangkat tersebut.	4	tidak bisa akses wifi pada area tertentu	1	Belum pernah terjadi kegagalan sistem	2	Berdasarkan laporan kerusakan	8	*Low*
21	Firewall		Tidak ada	8	Jika firewall mati bisa berakibat pada keamanan seluruh aset milik Universitas Muhammadiyah Yogyakarta	1	Belum pernah terjadi kegagalan sistem	1	Berdasarkan laporan kerusakan	8	*Low*
22	ASP .NET dan IIS		Tidak ada	1	No	1	No	1	No	1	*Low*

Tabel 3 Hasil Penilaian Aset Kritis

DISKUSI

Tujuan dari penelitian ini untuk menghasilkan profil ancaman aset kritis dan bobot nilai atas peluang terjadinya kegagalan dalam sistem, proses, serta produk maupun servis untuk menentukan tingkat keseriusan efek yang ditimbulkan yang ada di Universitas Muhammadiyah Yogyakarta. Hal-hal yang dilakukan pada pemberian nilai dari daftar aset mulai dari metode menggunakan OCTAVE, FMEA dan RPN. Pada bagian hasil penilaian aset kritis dapat dilihat bahwa mulai dari hardware, software dan data sudah diberi penilaian yang diukur dari severity, occurrence dan detection dan mendapatkan hasil RPN. Ada beberapa aset penting yang mungkin terlewat dari pencatatan maupun keterbatasan dalam wawancara. Keterbatasan dari segi daftar aset ini tidak semua ditampilkan, karena menyesuaikan dengan hasil wawancara yang dilakukan kepada Divisi Sistem Informasi Universitas Muhammadiyah Yogyakarta. Saran untuk perbaikan selanjutnya yaitu sering dilakukannya evaluasi untuk aset penting secara berkala yang ada di organisasi, dikarenakan untuk sekarang perbaikan hanya dilakukan jika terjadi kerusakan atau masalah saja dan juga Perihal penilaian risiko dengan ranking high memberi pengaruh yang begitu besar/banyak pada suatu perusahaan makadari itu risiko bisa di perkecil ataupun bisa dilakukan pencegahan sebelum terjadi kerusakan atau masalah.

KESIMPULAN

Pada penentuan aset teknologi informasi Universitas Muhammadiyah Yogyakarta penelitian ini menggunakan perhitungan RPN (Risk Priority Number) yang diambil dari perkalian severity, occurrence, detection yang memiliki nilai dari 1 sampai 10. Dari penilaian yang sudah dilakukan/dibuat dengan menggunakan metode Faillure Mode and Effect

(FMEA), control action risiko pada level risko very high dan high. Perihal ini dilakukan karena risiko dengan ranking very high dan high memberi pengaruh yang begitu besar/banyak pada suatu perusahaan makadari itu risiko bisa di perkecil ataupun bisa dilakukan pencegahan sebelum terjadi.

PENULISAN PUSTAKA DAN DAFTAR PUSTAKA

[1] A. F. Gary Stonebumer, Alice Goguen, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology," vol. 30, no. July, 2002.

[2] H. Azaim, "Pentingnya IT Risk Management Dalam Mendukung Keberlangsungan Bisnis," 2017. [Online]. Available: https://netsec.id/pentingnya-it-risk-management/.

[3] W. R. Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson, "Operationally Critical Threat, Asset, and Vulnerability Evaluations (OCTAVE(SM)) Framework, Version 1.0. Carnegie Mellon Software Engineering Institute," *Netw. Syst. Surviv. Progr.*, no. June, 1999.

[4] QAPI, "Guidance for Performing Failure Mode and Effects Analysis with Performance Improvement Projects," 2006.

[5] L. S. Lipol and J. Haq, "Risk analysis method : FMEA / FMECA in the organizations.," *Int. J. Basic Appl. Sci.*, vol. 11, no. 5, pp. 5–74, 2011.

[6] L. Obrand, N.-P. Augustsson, J. Holmstrom, and L. Mathiassen, "The Emergence of Information Infrastructure Risk Management in IT Services," *2012 45th Hawaii Int. Conf. Syst. Sci.*, pp. 4904–4913, 2012.

[7] Symantec, "IT RIs k Management," *Strategy*, vol. 2, no. December 2007, p. 52, 2008.

[8] Paul Hopkin, *Fundamentals of Risk Management Understanding, evaluating and implementing effective risk management*. 2010.

[9] S. P. L. M. Software, "How to conduct a failure modes and effects analysis," *A white Pap. issued by Siemens PLM Softw.*, 2016.

[10] A. Tarantino, "Failure Modes & Effects Analysis (FMEA) A Great Tool to Improve Product and Process Reliability and Reduce Risks." .

[11] A. Scangas, "FMEA F ailure Mode and Effects Analysis."

PENULIS: ADIKA MANDALA ARFIANDA YUHAZ

Adika Mandala Arfianda Yuhaz
Teknik Informatika, Teknik, Universitas Muhammadiyah Yogyakarta, Yogyakarta.
Email: adika.mandala.2014@ft.umy.ac.id