Mitigasi Risiko Aset Dan Komponen Teknologi Informasi Berdasarkan Kerangka Kerja OCTAVE Dan FMEA Pada Universitas Dian Nuswantoro

Risk Mitigation Asset And Information Technology Component Framework Based On OCTAVE And FMEA At The Dian Nuswantoro University

Gunawan Setyadi [1], Yupie Kusumawati [2]
[1,2] Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
[1,2]Jl. Nakula I, No. 5-11, Semarang, Kode Pos 50131, Telp. (024) 3520165 Fax: 3569684
E-mail : [1]112201204577@mhs.dinus.ac.id, [1]yupie@dsn.dinus.ac.id[2]

Abstrak

Mitigasi risiko merupakan pengambilan langkah – langkah untuk mengurangi kerugian yang dapat ditimbulkan dari dampak atas risiko. Karena wujud resiko belum diketahui secara jelas maka perlu adanya pengelolaan risiko secara baik dan benar agar tidak berdampak pada kelangsungan proses bisnis utama. Sering terjadinya kegagalan pada jaringan, terutama pada bagian server yang sering mengalami down pada saat KRS dan belum adanya prosedur yang memiliki standar keamanan dalam mengelola aset TI merupakan permasalahan yang selama ini dialami oleh Universitas Dian Nuswantoro. Maka dari itu tujuan dari penelitian ini adalah untuk mengetahui apa saja aset kritis di dalam organisasi, menganalisa dan mengevaluasi risiko, dan mengetahui langkah-langkah rencana mitigasi yang tepat terhadap aset TI. Metode penelitian yang digunakan yaitu Octave sebagai pengolah hasil informasi yang didapatkan dari wawancara. Dan FMEA digunakan untuk menghitung seberapa tinggi dampak untuk perusahaan jika risiko itu terjadi dan membuat ranking prioritas untuk masing-masing risiko. Dan hasil yang diperoleh didalam penelitian ini ada risiko yang berstatus very high 2 risiko, high 12 risiko, medium 13 risiko, low 23 risiko, very low 0 risiko. Sehingga dari hasil Risk Priority Number, yang perlu diberikan perhatian khusus yaitu Risk Priority Number yang memiliki status very high dan high.

***Kata kunci**: Mitigasi Risiko, Octave, FMEA, Aset Kritis, Ranking Prioritas*

Abstract

Risk mitigation could be interpreted as taking steps to reduce losses arising from the impact of such risks, because the manifestation of these risks are not certain yet. So it is needed to have a risk management that is good and right in order to not affect the main business processes. Frequent occurrence of failure on the network, especially on the server that is often experienced at a down moment during KRS ("Kartu Rencana Studi") and safety procedures which have not been standardized in managing IT assets are problem that have been experienced by the Dian Nuswantoro University. Thus, the purpose of this research was to determine what critical assets within the organization, to analyze and evaluate risks, and to determine the right mitigation actions steps toward IT assets. The method used were Octave, as the information processing result obtained from interviews. And FMEA, as a method to calculate how high the impact to the company if the risk happens and to rank the priorities for each risk. The results obtained in this study was that there was a risk that had very high 2 risk, 12 high risk, 13 medium risk, 23 low risk, very low 0 risk status. So that based on the Risk Priority Number, the risk which should be given special attention is the Risk Priority Number which has a vey high and high status.

***Keywords**: Risk Mitigation, Octave, FMEA, Critical Asset, Priority Ranking*

1. PENDAHULUAN

Berkembangnya teknologi informasi yang sangat pesat saat ini, menuntut hampir sebagian besar instansi pendidikan Indonesia bersaing kuat menciptakan pemanfaatan teknologi informasi. Teknologi informasi merupakan aset penting dalam mengelola dan menghasilkan informasi [1] yang bisa membuat perusahaan memiliki daya saing dan nilai tambah. Dengan memanfaatkan teknologi informasi, atas dasar prinsip penerapan ICT (*Information Communication Technologies*) dalam proses pembelajaran memungkinkan segala kegiatan yang berhubungan dengan informasi menjadi lebih mudah dan praktis. Namun seiring dengan manfaat yang diperoleh, teknologi informasi dalam penyelenggaraannya mengandung berbagai risiko.

Risiko adalah tantangan yang harus dihadapi di masa yang akan datang karena wujudnya yang belum diketahui secara pasti. Namun usaha untuk mengurangi atau memperkecil dampak yang ditimbulkan risiko, tetap dapat dilakukan dengan melakukan pengendalian risiko terhadap ketidakpastian [2]. Menurut Sancoyo Setiabudi, *Country Manager* untuk Cisco Indonesia "Tantangan dan risiko merupakan hal yang tidak dapat dihindari, terutama ketika berbicara mengenai kemajuan, pertumbahan, dan inovasi." Oleh sebab itu diperlukan penerapan manajemen risiko dalam menjalankan suatu proses bisnis utama dan pendukung. Agar dapat mengimplementasikan manajemen risiko yang esfisien dan efektif, diperlukan adanya keterlibatan dan pengawasan semua *stakeholder* dalam penyusunan penerapan kebijakan dan prosedur penggunaan teknologi informasi yang baik dan benar serta pengukuran untuk pengendalian dari risiko teknologi informasi yang berkesinambungan.

Universitas Dian Nuswantoro mempunyai banyak aktivitas utama dengan membagi aktivitas tersebut kedalam 2 bagian besar aktifitas utama, pertama yang dilakukan oleh PT. Dian Nuswantoro Teknologi dan Informasi (Dinustek) yang bertanggungjawab pada bagian *hardware* dan *network* sedangkan pada PSI (Pusat Sistem dan Informasi) bertanggung jawab pada bagian *software* dan *data*.

Disadari betul oleh pihak PT. Dian Nuswantoro Teknologi dan Informasi (Dinustek) dan PSI adanya risiko TI dan dampaknya yang mungkin muncul dalam penyelenggaraan unit pelaksanaan teknis jaringan komputer dan fasilitas pendukung yang ada di Universitas Dian Nuswantoro. Karena seringnya terjadi kegagalan pada jaringan terutama pada bagian server yang sering mengalami *down* pada saat proses pengisian kartu rencana studi (KRS) dan sering terjadi kegagalan atau kerusakan sistem dikarenakan *human error*. Sementara itu di Dinustek dan PSI belum ada prosedur terkait standar keamanan yang dimiliki dalam mengelola aset-aset TI. Sehingga dalam kegiatan operasional, manajamen jaringan komputer dan fasilitas pendukung yang ada pada Universitas Dian Nuswantoro perlu dilakukan pengelolaan risiko teknologi informasi.

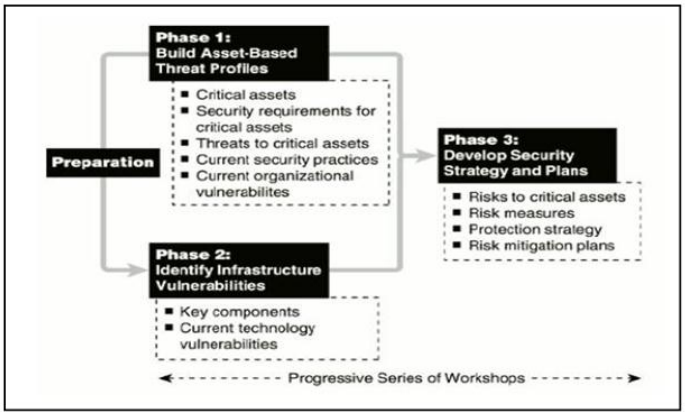
Pengelolaan risiko TI pada jaringan komputer dan fasilitas pendukung Dinustek dan PSI dengan menggunakan kerangka kerja *Octave* diharapkan dapat memberi idenfikasi yang jelas terkait aset kritis TI dan ancaman yang menimbulkan risiko TI, analisa dan evaluasi dari risiko TI yang mungkin muncul sehingga dapat memberi usulan strategi dan rencana implementasi manajemen risiko yang baik sesuai standar ISO 27001 dan 27002 dalam mengidentifikasi setiap *control* yang diperlukan untuk mengurangi risiko dan sejauh mana harus diterapkan.

2. METODE PENELITIAN

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan survei yaitu suatu cara penelitian *deskriptif* yang digunakan untuk menggambarkan atau memotret masalah yang terkait dengan risiko yang ada pada organisasi.

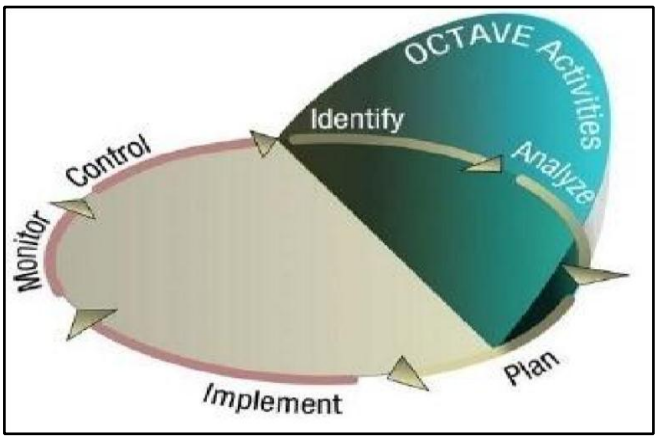
2.1 Dasar Teori

Ada banyak kerangka kerja yang dapat digunakan perusahaan dalam penerapan manajemen risiko. Salah satu diantara banyak kerangka kerja yang ada dipilih *Operationally Critical Threat, Asset and Vulnerability Evaluation* (OCTAVE) sebagai kerangka kerja yang dapat mengidentifikasi, menganalisa dan mengawasi pengelolaan risiko keamanan informasi [3].



Gambar 1. Fase OCTAVE

Setelah mengetahui tahapan dari metode octave selanjutnya mengetahui proses yang ada didalam octave :



Gambar 2 . Proses Octave [3]

Untuk melengkapi proses analisa dari risiko TI, dipilih FMEA (*Failure Mode and Effect Analysis*) sebagai prosedur dalam penilaian risiko TI yang akan dan mungkin dihadapi, dengan memberitahukankan tentang informasi dasar mengenai kendala risiko, proses, dan desain.

FMEA secara sistematis membantu untuk mengidentifikasi dan menilai (*mode*), penyebab (*cause*), dan dampak (*effect*) dari kegagalan suatu sistem sebelum itu terjadi. Hasil analisis dan penilaian tersebut akan membentuk peringkat dari setiap kegagalan sesuai dengan tingkat efek risiko dan probabilitas terjadinya.

2.2 Jenis Data

Penelitian ini menggunakan jenis data kualitatif yaitu data yang cenderung bersifat *deskriptif* serta cenderung pada analisis. Data kualitatif diperoleh melalui berbagai macam teknik pengumpulan data seperti analisa dokumen, wawancara, diskusi, atau observasi. Dan dalam penelitian ini data kualitatif mengacu pada penggunaan metode octave. Karena metode octave sesuai digunakan untuk menganalisa asset-aset IT pada organisasi.

2.3 Sumber Data

Sumber data yang digunakan dalam penelitian ini adalah :

1. Data primer adalah data yang diperoleh langsung dari responden. Data primer penelitian ini diperoleh langsung dari karyawan / pegawai Universitas Dian Nuswantoro tepatnya pada bagian yang menangani komponen-komponen TI yaitu pada Dinustek dan PSI. Dari data primer didapatkan faktor ancaman apa saja yang dihadapi oleh Universitas Dian Nuswantoro.
2. Data sekunder adalah data yang diperoleh tidak langsung dari responden. Data sekunder dalam penelitian ini adalah data dari referensi buku dan jurnal yang barkaitan dengan keamanan asset dan komponen TI.

2.4 Metode Analisis Yang Digunakan

Metode analisis yang digunakan dalam penelitian ini menggunakan dua metode yaitu :

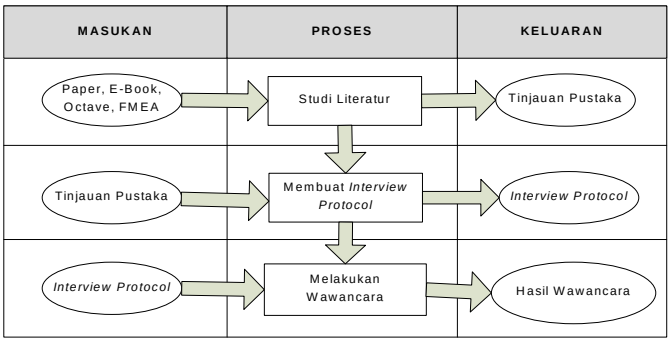
1. Metode OCTAVE yang digunakan untuk mengolah data hasil wawancara.
2. Metode FMEA yang digunakan untuk memberikan nilai pada setiap komponen–komponen teknologi informasi yang sudah didefinisikan pada metode octave.

2.5 Langkah - Langkah Penelitian

Metodologi penelitian digambarkan dalam bentuk alur diagram, dimana diagram menggambarkan urutan proses secara mendetail dan hubungan antara satu proses dengan proses lainnya. Berikut adalah paparan alur diagram dari metodologi penelitian yang dilakukan di tiap fase:

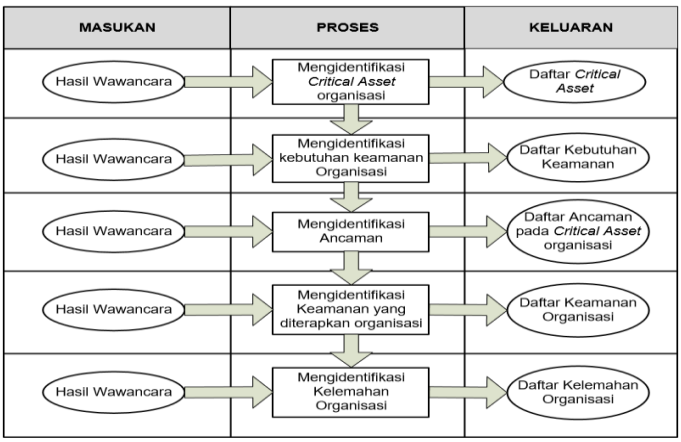
1. Studi literatur yang di lakukan menggunakan beberapa sumber baik buku fisik maupun *paper*, *e-book*, jurnal yang didapatkan secara online. Tujuan dari melakukan studi literatur adalah untuk mendapatkan pemahaman dan wawasan mengenai manajemen risiko TI dan kerangka kerja yang digunakan dalam melakukan penilaian risiko dan mitigasi terhadap risiko tersebut.
2. Membuat *interview protocol* Pemahaman dan wawasan yang dimiliki dari proses melakukan studi literatur sebelumnya , menjadi dasar untuk membuat *interview protocol* yang berisi mengenai daftar pertanyaan yang akan diajukan kepada pihak perusahaan.

Tabel 1 Fase 0 *Preparation* Kerangka Kerja Octave



3. Melakukan wawancara tujuan dari melakukan wawancara adalah untuk menggali informasi mengenai organisasi. Dan di penelitian kali ini mewawancarai *staff* sistem *administrator*, dan *network admin* Dinustek dan Kepala PSI, untuk mengetahui aset-aset atau fasilitas yang ada pada Universitas Dian Nuswantoro, kebutuhan keamanan, ancaman, komponen utama, dan evaluasi komponen.

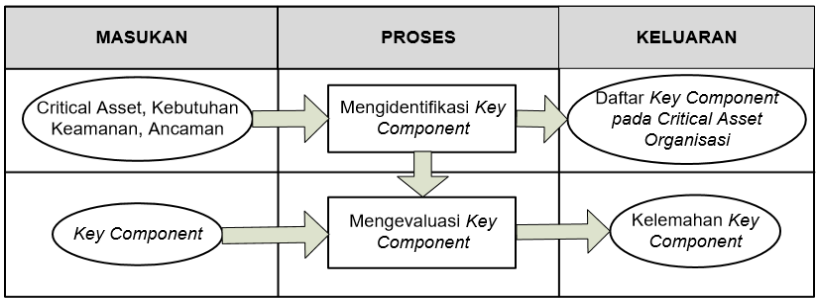
Tabel 2 Fase 1 *Organizational View* Kerangka Kerja Octave



1. Mengidentifikasi *Critical Asset* Perusahaan, dari hasil wawancara yang sudah dilakukan dengan pihak terkait, maka akan didapatkan informasi mengenai *critical asset* yang dimiliki oleh perusahaan.
2. Mengidentifikasi Kebutuhan Keamanan Perusahaan, dari hasil wawancara yang sudah dilakukan, maka akan didapatkan informasi mengenai kebutuhan keamanan pada perusahaan.
3. Mengidentifikasi Ancaman, dengan menganalisis hasil wawancara dan daftar kebutuhan keamanan yang ada pada perusahaan, maka dapat dilakukan identifikasi terkait ancaman pada setiap *critical asset*.
4. Mengidentifikasi keamanan yang sudah diterapkan perusahaan, melakukan wawancara untuk mengidentifikasi keamanan yang diterapkan oleh perusahaan. Hasil dari proses ini adalah daftar keamanan yang sedang diterapkan perusahaan.

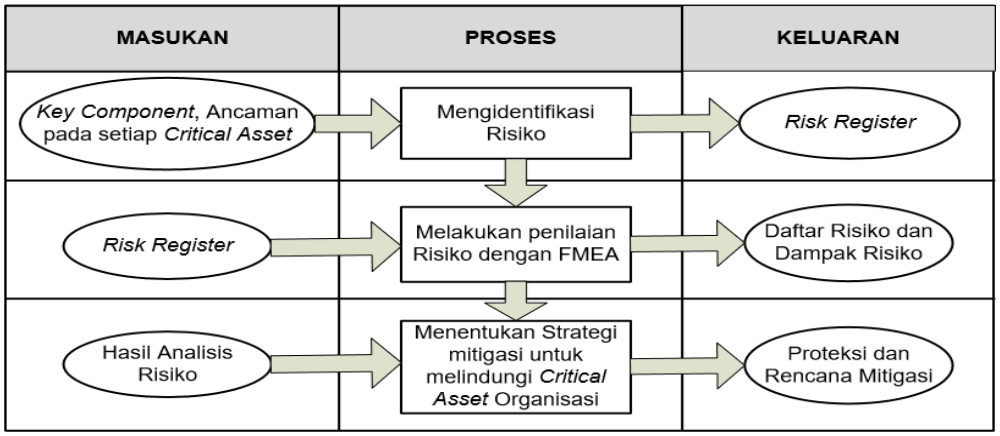
5. Mengidentifikasi Kelemahan Perusahaan, melakukan wawancara untuk mengidentifikasi kelemahan yang dimiliki oleh perusahaan.

Tabel 3 Fase 2 *Technological View* Kerangka Kerja Octave



1. Mengidentifikasi *Key Components*, dari daftar *critical asset*, kebutuhan keamanan perusahaan dan ancaman yang didapat dari proses wawancara, selanjutnya akan dilakukan analisis dan idenfitikasi mengenai *key components* dari setiap *critical assets*.
2. Mengevaluasi *Key Components*, setelah mendapatkan daftar *key components* setiap *critical assets* maka selanjutnya akan dilakukan evaluasi untuk menemukan kerentanan atau kelemahan dari setiap *key components*.

Tabel 4 Fase 3 *Strategy and Plan*



Pengembangan Kerangka Kerja Octave :

1. Mengidentifikasi risiko, pada tahap ini akan mengidentifikasi risikorisiko yang mungkin terjadi terkait dengan *critical asset*. Risiko yang akan diidentifikasi berupa risiko yag pernah terjadi maupun perkiraan terhadap risiko yang mungkin terjadi di masa yang akan datang
2. Melakukan Penilaian Risiko dengan Metode FMEA, dalam melakukan penilaian terhadap risiko dibutuhkan sebuah kerangka kerja agar penilaian yang dilakukan obyektif dan terpercaya. Pada tugas akhir ini digunakan kerangka kerja FMEA untuk melakukan penilaian risiko. Penilaian risiko menggunakan FMEA didasarkan pada tiga faktor, yaitu :
   a. *Risk Severity*, digunakan untuk menganalisa risiko dengan menghitung seberapa besar dampak kejadian mempengaruhi output proses.

b. *Risk Occurance*, menunjukan seberapa sering / intensitas risiko terjadi, serta menjabarkan skala pengukuran risiko berdasarkan peluang terjadinya.

c. *Risk Detection*, adalah pengukuran terhadap kemampuan mengendalikan atau mengontrol kegagalan yang dapat terjadi.

Setelah mendapatkan nilai dari setiap faktor *severity, occurance* dan *detection,* kemudian nilai tersebut akan dikalikan sehinga menghasilkan sebuah nilai *Risk Priority Number*.

RPN = *Sev* x *Occur* x *Detec.* .....(1)

Dari nilai RPN selanjutnya dikategorikan berdasarkan tingkat risiko yang ada.

3. Menentukan strategi mitigasi untuk melindungi asset kritis perusahaan Pada tahap ini akan diidentifikasi langkah mitigasi risiko berdasarkan ISO 27001 dan 27002, yaitu sesuai dengan panduan *Guide to Risk Assessment & Respons,* Agustus : 2012 yaitu *Avoidance* Menghindari risiko untuk terjadi bagaimanapun caranya. *Transfer* Membiarkan orang lain mengambil risiko (misalnya. oleh asuransi atau untuk kontraktor lewat tanggung jawab untuk risiko). *Limitation / Mitigation* Menerima risiko tetapi berupaya untuk mengurangi atau membatasi dampak dari risiko. *Acceptance* Menerima Risiko.

3. HASIL DAN PEMBAHASAN

Dari penelitian yang dilakukan, didapatkan banyaknya aset TI yang memiliki risiko yang tinggi. Berikut merupakan jumlah hasil penilaian risiko berdasarkan level *Risk Priority Number*:

Tabel 5: Jumlah hasil penilaian risiko

Level RPN	Jumlah
Very High	2 Risiko
High	12 Risiko
Medium	13 Risiko
Low	23 Risiko
Very Low	0 Risiko

Dan dari hasil penelitian yang menghasilkan aset TI dengan *Risk Priority Number* seperti tabel 5, selanjutnya melakukan mitigasi risiko terhadap aset TI. Sesuai dengan panduan *Guide to Risk Assessment & Respons,* Agustus : 2012, Mitigasi risiko ada 4 macam yaitu *Avoidance* Menghindari risiko untuk terjadi bagaimanapun caranya. *Transfer* Membiarkan orang lain mengambil risiko (misalnya. oleh asuransi atau untuk kontraktor lewat tanggung jawab untuk risiko). *Limitation / Mitigation* Menerima risiko tetapi berupaya untuk mengurangi atau membatasi dampak dari risiko. *Acceptance* Menerima Risiko. Berikut merupakan jumlah hasil mitigasi risiko :

Tabel 6 Jumlah hasil mitigasi risiko

Mitigasi	Jumlah
Transferred	5 Risiko
Limitation	33 Risiko
Acceptance	7 Risiko
Avoidance	11 Risiko

Setelah mitigasi resiko didapatkan dengan berdasarkan ISO 27001/27002 menjelaskan mengenai pemberian *control objective* sesuai dengan penyebab masing-masing dari risiko. Berikut ini adalah *control objective* dari risiko-risiko dengan level sangat tinggi (*Verry High*) dan tinggi (*High*).

ID Resiko	D04
Kategori	Data
Resiko	Pembobolan Database
Penyebab	Tingkat Keamanan Database Masih Kurang
Control Objevtive	7.2.1-*Management responsibilities* Udinus harus memastikan karyawan untuk sadar dan memenuhi tanggung jawab keamanan informasi 7.2.2-*Information Information security awareness education, and training* Seluruh karyawan di dalam Udinus harus diberikan pelatihan kesadaran yang tepat dalam melindungi asset-aset TI milik udinus dan selalu diingatkan mengenai kebijakan dan prosedur yang sesuai dengan pekerjaan mereka. Jika melanggar, maka harus ada langkah tegas dari pihak manajemen 7.2.3-*Disciplinary process* Harus adanya proses pendisiplinan secara formal dan komunikatif secara langsung saat terjadi aksi pelanggaran keamanan informasi 12.2.1-*Controls againt malware* Control deteksi, pencegahan, dan *recovery* dalam melawan malware harus diimplementasikan oleh udinus, dan dikombinasikan dengan kesadaran para penggunanya. 13.1.1-*Network Controls* Semua jaringan di dalam udinus, baik jaringan internet, telekomunikasi, dan sejenisnya harus dikelola dengan baik 13.1.3-*Segregation in networs* Layanan informasi, pengguna, dan sistem informasi harus dipisahkan di dalam jaringan dan disesuaikan dengan keperluan

Implementation	tiap karyawan atau *staff* dalam bekerja - Meningkatkan sistem keamanan jaringan dan database - Membedakan TCP/IP database atau server dengan sistem lain - Koneksi sistem ke dalam jaringan database harus dibatasi - Harus ada otentikasi jika ada sistem atau pengguna yang ingin mengakses database - Pihak yang memiliki akses saja yang dapat mengakses data yang berada di dalam database - Divisi *network* memastikan karyawan mengerti tentang tanggung jawab mereka terhadap keamanan aset informasi yang ada di Udinus - Memberikan petunjuk *guideline* keamanan aset informasi

4. KESIMPULAN

Berdasarkan hasil penelitian yang sudah dilakukan terkait dengan mitigasi risiko yang menangani aset-aset kritis pada Universitas Dian Nuswantoro, maka bisa diambil kesimpulan seperti dibawah ini :

1. Dalam menetapkan penilaian terhadap aset kritis yang dimiliki Universitas Dian Nuswantoro penelitian ini menggunakan perhitungan *Risk Priority Number* yang diambil dari perkalian 3 variabel yaitu *Severity* (keparahan), *Occurance* (intensitas), dan *Detection* (deteksi risiko) yang memiliki *value* dari 1 hingga 10.

   Pemberian *value* tersebut berdasarkan kondisi kekinian aset kritis Universitas Dian Nuswantoro. Sehingga semakin tinggi *Risk Priority Number* maka semakin berpengaruh mengganggu proses bisnis utama Universitas Dian Nuswantoro.

2. Dalam penilaian penelitian ini terhadap aset kritis yang memiliki level *Risk Priority Number* yang tinggi seperti *Very High* dan *High* adalah jenis aset-aset yang harus diberi perhatian khusus seperti risiko yang memiliki ID : D04, H03 (*Very High*) dan S01, D01, D05, H19, H05, H09, H16, N01, H18, H36, S02, P01 (*High*). Dan setelah risiko yang telah disebutkan diatas baru Universitas Dian Nuswantoro dapat membagi perhatiannya dengan risiko yang berlevel *medium*, *Low*, dan *Very Low*.

5. SARAN

Adapun saran yang dapat disampaikan peneliti untuk perbaikan penelitian lanjutan pada masa mendatang, yaitu :

1. Melakukan penelitian dengan menggunakan metode berbeda maupun mengacu pada standar ISO yang berbeda supaya didapatkan variasi hasil yang berbeda pula.
2. Peneliti selanjutnya perlu melakukan wawancara dan membagi kuesioner pada semua *stackholder* yang menangani bagian IT yang ada di Universitas Dian Nuswantoro tentunya agar bisa mendapatkan informasi yang sesuai dengan kondisi sesungguhnya.

DAFTAR PUSTAKA

[1] R.E. Indrajit, "Manajemen Sistem Informasi dan Teknologi Informasi, " Pengantar Konsep Dasar, 2000. [2] Muslich, "Pengukuran Risiko," Depok, 2007.

[3] C Albert, A Dorofee, J Stevens, and C Woody, "Introduction to the OCTAVE, "Networked Systems Survivability Program, 2003.

[4] L.N. Wati and Mamduh Hanafi, "Manajemen Risiko Bisnis," Jurnal Ekobis, p. 256, 2009.

[5] Harold. (2010) Identifikasi Risiko Berdasarkan ISO/IEC 31000:2009. [Online]. https://reycca.wordpress.com/2013/04/22/identifikasi-resiko/

[6] Shift Indonesia. (2012, juni) shift. [Online]. http://shiftindonesia.com/leansix-sigma-mengenal-metode-fmeafailure-mode-and-effects-analysis/

[7] C.S. Carlson, "Understanding and Applying the Fundamentals of FMEAs," 2014.

[8] Mattord and Dr. Michael E. Whitman, Principles of Information Security. Australia, Brazil, Japan, Korea, Mexico, Singapore, Spain, United Kingdom, United States: Course Technology, 2011.

[9] R. Iffano Sarno, "Audit Keamanan Sistem Informasi Berdasarkan Standar ISO," p.2, 2009.

[10] eman Setiawan, "Etika dan Profesionalisme," KAI, p. 2, 2011.

[11] Badan Standardisasi Nasional, "Teknologi Informasi - Teknik Keamanan - Sistem Manajemen Keamanan Informasi - Persyaratan," in Standar Nasional Indonesia.: Badan Standardisasi Nasional, 2014, p. 7.

[12] Training ISO & Consulting Sintegral. (2013, September) Sintegral. [Online]. http://sintegral.com/iso27001-kemanan-informasi/

[13] ISO/IEC 27001, "Infomation technology-Security techniques Information Security Management System-Requirements," International Standard, October 2013.

[14] ISO/IEC 27002, "Infomation technology-Security techniques-code of practice for information security controls," International Standard, October 2013.