Analisis dan Mitigasi Risiko Aset Kritis Terhadap Kegagalan Proses Produksi Penyiaran Di TVKU Semarang Menggunakan Metode OCTAVE Dan FMEA

Analysis and Mitigation of Critical Asset Risk on The Failure of Process of Broadcasting Production in TVKU Semarang Using OCTAVE And FMEA Method

Annisa Nafasari[1], Wellia Shinta Sari[2]
[1,2]Jurusan Sistem Informasi, Universitas Dian Nuswantoro, Semarang
Jl. Imam Bonjol No. 27, Semarang, Kode Pos 50131, Telp (024) 3520165, Fax: 356984
e-mail: [1]annisanafasari25@gmail.com, [2]wellia.shinta@dsn.dinus.ac.id

Abstrak

TVKU (Televisi Kampus Udinus) merupakan sebuah stasiun televisi lokal Semarang yang berlokasi di dalam kawasan kampus Universitas Dian Nuswantoro, yang setiap harinya selalu memproduksi berita terbaru, iklan dan acara-acara harian lainnya baik secara live maupun tapping. Dalam menjalankan proses bisnisnya banyak risiko-risiko terjadi yang membuat terganggunya proses bisnis, misalnya server n-computing dan server streaming (virtual) yang mengalami overheat, kurangnya proses controlling dan maintenance pada server, kabel video yang rusak dan penyalahgunaan hak akses. Oleh karena itu, untuk mencapai tujuan dan menjalankan proses bisnisnya maka perlu dilakukan adanya suatu manajemen risiko untuk mengarahkan dan mengendalikan risiko yang suatu saat terjadi. Tujuan dari penelitian ini adalah untuk mengidentifikasi, menilai, dan melakukan mitigasi risiko yang berkaitan dengan aset kritis yang mendukung proses produksi penyiaran di TVKU Semarang dengan menggunakan metode OCTAVE sebagai pengolah hasil informasi yang didapatkan dari wawancara dan menggunakan metode FMEA untuk menghitung seberapa tinggi dampak masing-masing risiko bagi perusahaan serta menggunakan pedoman kontrol IS0 27002:2013. Hasil yang diperoleh dari penelitian ini yaitu terdapat 73 risiko dengan 4 risiko very high, 8 risiko high, 14 risiko medium, 25 risiko low dan 22 risiko very low, setelah itu maka dilakukan rekomendasi langkah mitigasi risiko pada masing-masing risiko aset kritis dan melakukan rekomendasi menggunakan pedoman kontrol ISO 27002:2013 pada risiko aset kritis yang memiliki level risiko very high dan high.

Kata kunci—Mitigasi Risiko, Aset Kritis, Octave, FMEA, ISO27002:2013

Abstract

TVKU (Udinus Campus Television) is a local television station Semarang located in the campus area of Dian Nuswantoro University, which every day always produce latest news, advertisement and other daily events both live and tapping. In running the business process many risks occur that make the business process disrupt, such as server n-computing and server streaming (virtual) that overheated, lack of controlling and maintenance process on the server, broken video cable and abuse of access rights. Therefore, to achieve the objectives and run the business process it is necessary to do a risk management to direct and control the risk that one day occurred. The purpose of this study is to identify, assess and mitigate risks associated with critical assets that support the broadcast production process at TVKU Semarang using the OCTAVE method as a processor of information obtained from interviews and using the FMEA method to calculate how high the impact of each each risk for the company and using IS0 27002: 2013 control guidelines. The result of this research is that there are 73 risks with 4 very high risk, 8 high risk, 14 medium risk, 25 low risk and 22 very low risk, after which recommendation of risk mitigation step at each risk of critical asset and doing

recommendations using the ISO 27002: 2013 control guideline on the risk of critical assets with very high and high risk levels.

Keywords—Risk Mitigation, Critical Assets, Octave, FMEA, ISO27002: 2013

1. PENDAHULUAN

Kebutuhan teknologi informasi (TI) mengalami peningkatan yang semakin tinggi, seperti pemanfaatan teknologi informasi yang digunakan untuk menjalankan aktifitas-aktifitas penting dan banyak memberikan kemudahan pada berbagai aspek kegiatan bisnis [1]. Teknologi informasi merupakan aset penting dalam mengelola dan menghasilkan informasi yang bisa membuat perusahaan memiliki daya saing dan nilai tambah[2]. Demi tercapainya hal tersebut, maka perlu ditunjang dengan pengelolaan teknologi informasi yang memadai supaya teknologi informasi mampu menyukseskan perusahaan dalam mencapai tujuan bisnisnya.

Banyak perusahaan yang memanfaatkan teknologi informasi untuk proses bisnisnya dan tentunya di perusahaan tersebut menghadapi suatu permasalahan baik internal atau eksternal dalam mencapai tujuan bisnisnya. Begitu pula pada stasiun televisi, stasiun televisi sebagai penyelenggara layanan yang memberikan informasi dalam bentuk audio dan video setiap harinya. Oleh karena itu, stasiun televisi membutuhkan dukungan teknologi informasi untuk mengelola dan menyajikan informasi kepada masyarakat umum. Salah satu stasiun televisi yang memanfaatkan teknologi informasi sebagai berlangsungnya proses bisnis yaitu TVKU (Televisi Kampus Udinus) Semarang.

TVKU (Televisi Kampus Udinus) merupakan sebuah stasiun televisi lokal Semarang yang berlokasi di dalam kawasan kampus Universitas Dian Nuswantoro. Setiap harinya TVKU selalu memproduksi berita terbaru, iklan dan acara-acara harian lainnya baik secara *live* maupun *tapping*, sebelum menjadi suatu program acara yang siap ditayangkan, tentunya sebelumnya dilakukan suatu proses *editing*, proses tersebut juga memerlukan dukungan teknologi informasi untuk mengolah informasi yang akan diberikan pada masyarakat. Dalam penggunaannya terkadang mengalami suatu permasalahan dan hambatan yang menyebabkan suatu kegiatan penyiaran mengalami gangguan. Misalnya kehilangan data, kabel video atau perangkat *broadcasting* rusak, tidak ada jaringan internet saat *live*, bencana alam atau suatu ancaman keamanan lainnya yang membuat kegagalan dalam melakukan penyiaran. Apalagi stasiun televisi setiap harinya harus melakukan penyiaran berita, iklan dan acara-acara harian lainnya untuk diberikan kepada masyarakat, yang dilakukan penjadwalan dalam penyiarannya juga, jika suatu proses penyiarannya mengalami gangguan dan terjadi kegagalan dalam menyiarkan maka akan fatal dan tidak dapat menyiarkan acara tersebut dan akan berdampak merugikan terhadap TVKU. Adanya kemungkinan terjadinya permasalahan-permasalahan terkait penerapan itulah yang mendasari pentingnya melakukan analisis risiko terkait penerapan aset kritis yang mendukung proses produksi penyiaran di TVKU Semarang.

Risiko merupakan suatu keadaan yang wujudnya belum terjadi, dimana jika terjadi maka akan menimbulkan kerugian di masa yang akan datang. Namun usaha untuk mencegah terjadinya risiko dapat dilakukan yaitu dengan menerapkan mitigasi risiko yang sebelumnya dilakukan analisis dan identifikasi risiko agar dapat mengetahui risiko-risiko apa saja yang mungkin akan terjadi [3]. Maka untuk mengidentifikasi dan menganalisis risiko aset kritis yang mendukung proses produksi di TVKU diterapkan metode OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*) dan untuk melengkapi proses analisa diterapkan metode FMEA (*Failure Mode and Effect Analysis*) sebagai prosedur penilaian risiko yang akan didapatkan nilai RPN dari yang tertinggi hingga terkecil untuk risiko sekarang atau yang akan datang. Kemudian menerapkan suatu kontrol ISO 27002:2013, sehingga dapat memberi usulan strategi dan rencana implementasi mitigasi risiko yang baik agar dapat mengurangi risiko yang mungkin akan terjadi.

Berdasarkan penjelasan diatas, tujuan penelitian ini adalah untuk melakukan identifikasi risiko aset kritis pada proses produksi penyiaran di TVKU Semarang dan memberikan masukan bagaimana langkah mitigasi risiko yang tepat sesuai dengan hasil analisis dan identifikasi risiko

yang akan terjadi. Hasil yang ingin dicapai penulis pada penelitian tugas akhir ini adalah suatu pedoman yang dapat menangani permasalahan yang terjadi atau akan terjadi yang berupa sebuah dokumen analisis mitigasi risiko pada aset kritis yang mendukung proses produksi di TVKU Semarang. Oleh karena itu penulis memberikan judul "Analisis Dan Mitigasi Risiko Aset Kritis Terhadap Kegagalan Proses Produksi Penyiaran Di Tvku Semarang Menggunakan Metode OCTAVE dan FMEA".

2. METODE PENELITIAN

Pada Penelitian ini metode pengambilan data yang digunakan adalah dengan studi literatur dan wawancara. Metode analisis yang digunakan yaitu metode OCTAVE dan Metode FMEA. Metode OCTAVE digunakan untuk mengolah hasil dari wawancara serta sebuah teknik atau metode yang digunakan sebagai kerangka kerja yang dapat mengidentifikasi, menganalisa dan mengawasi pengelolaan risiko keamanan informasi berdasarkan pengidentifikasian risiko [4], Metode OCTAVE memiliki beberapa fase, diantaranya :

Fase 0 : Melakukan persiapan dengan menyusun jadwal, membentuk tim analisis, meminta dukungan dan menyiapkan logistik.

Fase 1 : Membangun profil ancaman berdasarkan aset yang ada di organisasi

Fase 2 : Mengidentifikasi Kerentanan Infrastruktur

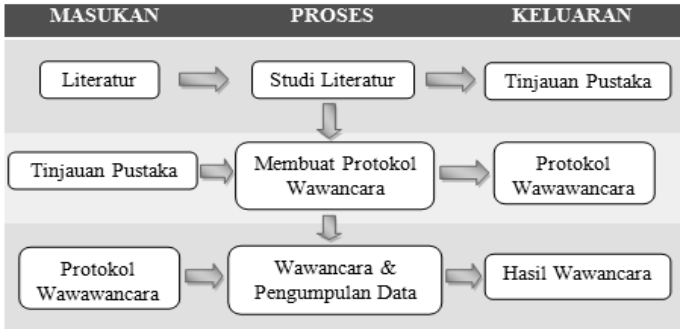
Fase 3 : Mengembangkan rencana dan strategi keamanan

Metode FMEA yaitu suatu metode yang terstruktur yang dapat digunakan untuk mengidentifikasi, memprioritaskan mode kegagalan (*failure mode*) kemudian mencegahnya sebanyak mungkinserta memberikan penilaian risiko aset kritis yang mendukung proses produksi penyiaran yang telah terdefinisi dengan metode OCTAVE, yang akan didapatkan nilai risiko dari yang tertinggi hingga terkecil[5]. Metode FMEA memiliki beberapa tahapan, diantaranya[6] :

1. Identifikasi ruang lingkup dari konsep FMEA yang akan dibuat
2. Mengidentifikasi kegagalan dan efeknya
3. Menentukan tingkat keparahan efek dari suatu kegagalan (Severity)
4. Menentukan Occurrence
5. Menentukan Deteksi (Detection)
6. Menghitung RPN, RPN = S x O x D
7. Menentukan level risiko paling tinggi berdasarkan nilai RPN
8. Mengambil tindakan untuk mengurangi atau menghilangkan risiko tertinggi / risiko kritis.

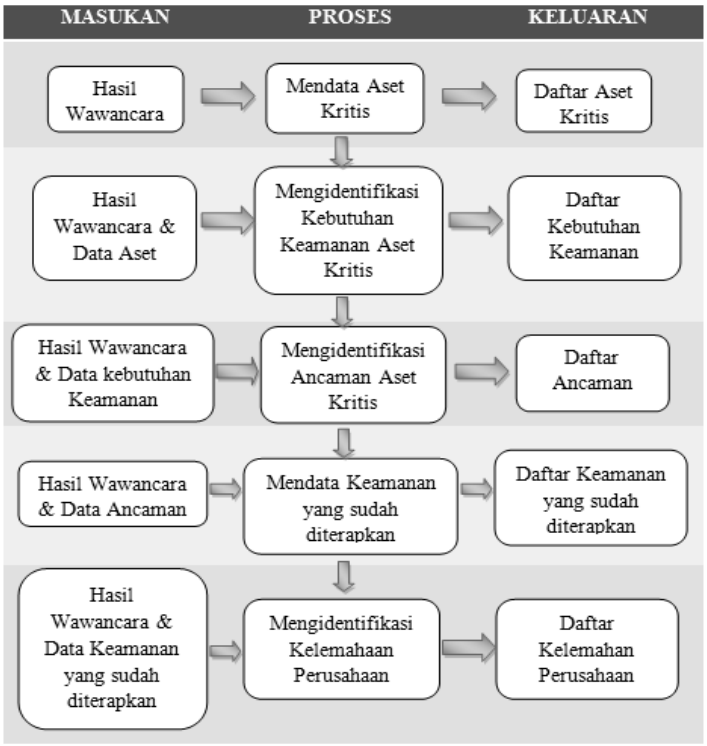
Metode penelitian akan digambarkan dalam suatu diagram alur, yang menggambarkan urutan proses secara detail dan hubungan satu proses dengan proses lainnya, berikut diagram alur penelitian ini :

a. Fase Persiapan.



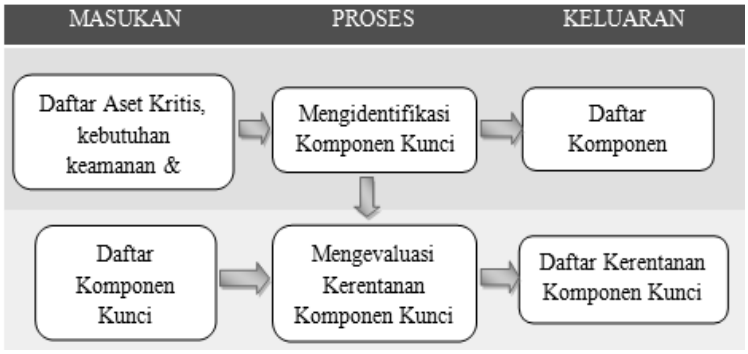
Gambar 1. Fase Persiapan

b. Fase 1 : Membangun profil ancaman berdasarkan aset yang ada di organisasi.



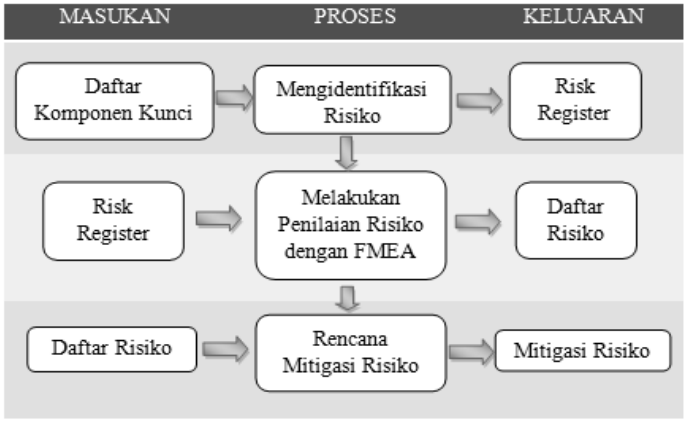
Gambar 2. Perancangan Profil Ancaman

c. Fase 2 : Mengidentifikasi kerentanan infrastruktur.



Gambar 3. Identifikasi Kerentanan Infrastruktur

d. Fase 3 : Mengembangkan rencana dan strategi keamanan.



Gambar 4. Pengembangan Rencana dan Strategi Keamanan

3. HASIL DAN PEMBAHASAN

a. Identifikasi Aset Kritis

Tabel 1. Identifikasi Aset Kritis

Kategori Aset	Aset Kritis	
Hardware	• Router Mikrotik RB1100AHx • Kamera • Server n-computing (virtual) • Server penyimpanan • Server Active Direktory • Kabel Jaringan • UPS • Microwave jaringan • PC • Modem • Encoder • Decoder • ATEM BlackMagic	• DVD • Hyperdeck • Mixer Audio • Kabel Video • Transmitter • Genset • Switch • Server Streaming • CCTV • Mesin RFID Card • Lighting • Mikrofon
Software	• Adobe Premiere • Adobe After Effect • Software CG	• Software Vmix • Insta Playout
Network	• Jaringan Internet • Jaringan Intranet	
People	• Divisi IT • Produksi	• Divisi Teknik
Data	• Data Karyawan • Data Keuangan	• Data Inventory Alat • Data Rekaman Video
Procedure	• SOP IT • SOP Produksi	• SOP Teknik

b. Ancaman pada Aset Kritis

Tabel 2. Ancaman Aset Kritis

Aset Kritis	Ancaman
Router Mikrotik RB1100 Ahx, Switch	• Manipulasi konfigurasi pada perangkat • Perangkat rusak
Kamera	• Kamera rusak disebabkan karena umur • Hilangnya kamera
Server n-computing, Server Streaming (Virtual)	• Server *hang*/*down* • Server mati • Server rusak • Kesalahan Konfigurasi • Adanya bencana alam
Server penyimpanan	• Hardisk rusak • Adanya pencurian data

Aset Kritis	Ancaman
	• Server down • Server rusak • Server mati • Adanyabencanaalam
Server Active Direktory	• Server rusak • Server mati • Adanya bencana alam
Kabel Jaringan	• Kabel rusak
UPS, Genset	• Perangkat rusak • Hilangnya perangkat • Perangkat tidak berfungsi normal
Microwave jaringan	• Tersambar petir • Microwave jaringanRusak
PC	• Adanya virus • Pencurian PC • Kerusakan Perangkat • Penyalahgunaan hak akses • Adanya bencana alam
Transmitter	• Rusak • Adanya bencana alam
CCTV	• CCTV rusak • *Hardware* mati
Mesin RFID *card*	• Mesin RFID card hilang • Mesin RFID card rusak • Hardware mati
Lighting	• Perangkat rusak
Mikrofon	• Perangkat rusak • Perangkat hilang
Adobe Premiere, Adobe After Effect	• *Software hang*
Software Vmix, Software CG, Insta Playout	• *Software hang*
Jaringan Internet	• Jaringan internet tidak dapat digunakan
Jaringan Intranet	• Terputusnya jaringan komputer antara satu unit dengan unit lain.
Divisi IT, Produksi dan Teknik	• Tidak mampu mengatasi masalah dengan tepat dan cepat • Penyalahgunaan hak akses
Data Karyawan, Data Keuangan, Data Inventory Alat, Data Rekaman Video	• Pencurian data • Penyalahgunaan wewenang • Kehilangan data akibat bencana alam • Data tidak bisa diakses

Aset Kritis	Ancaman
	• Redundasi data
SOP IT, Produksi, Teknik	• Operasional perusahaan tidak berjalan dengan efektif dan efisien pada SOP perawatan server, SOP penyimpanan data video, dan SOP perawatan alat siaran.
Encoder dan Decoder	• Perangkat rusak • Perangkat hilang • Kesalahan konfigurasi • Perangkat rusak
Modem, ATEM BlackMagic, DVD, Hyperdeck, Mixer Audio	• Perangkat hilang • Kabel rusak
Kabel Video	• Kabel rusak

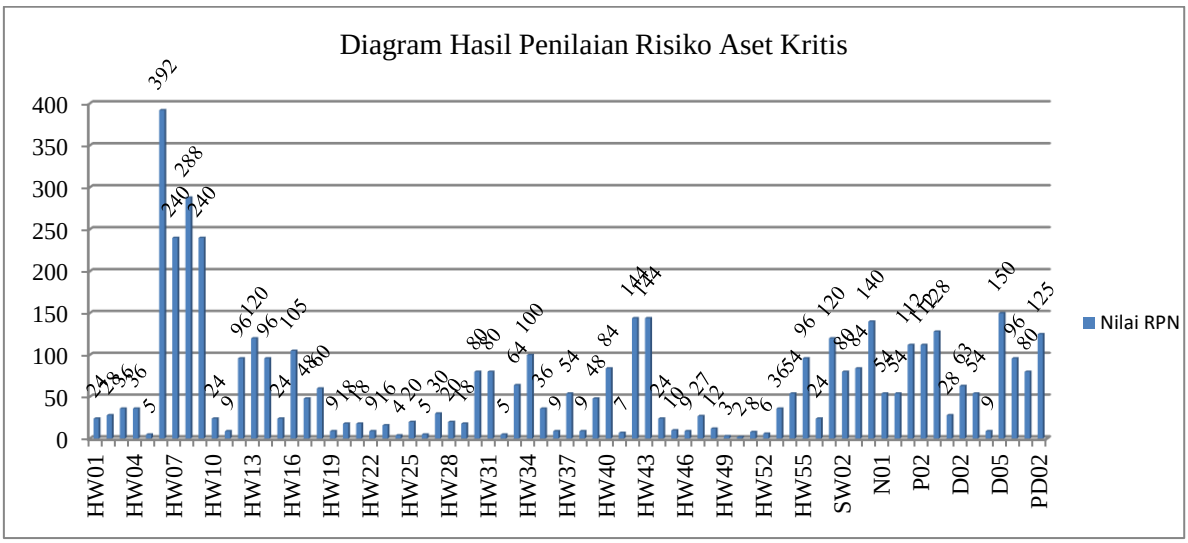
c. Keamanan yang telah diterapkan.

1. Pemasangan mesin *RFID card* di perusahaan
2. Pemasangan CCTV
3. Pelatihan Karyawan
4. Backup data
5. Pembatasan hak akses
6. Ruang pendingin untuk *server*
7. Pemasangan *Firewall*
8. Menggunakan antivirus berlisensi

d. Kelemahan Perusahaan.

1. Kurang rutin mengontrol atau merawat perangkat
2. Belum adanya *backup* listrik atau *genset* di pemancar Masjid Agung Jawa Tengah
3. Terbatasnya alat yang dimiliki perusahaan sehingga terkadang ada alat yang harus menyewa diluar.
4. Kekurangan sumberdayamanusia yang memadai.

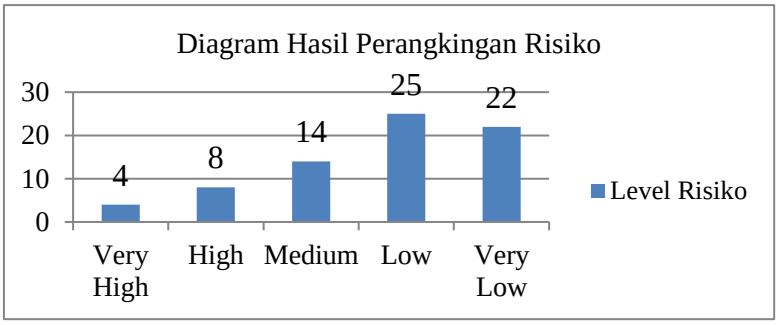
e. Hasil Penilaian Tingkat Risiko Aset Kritis



Gambar 5. Hasil Penilaian Tingkat Risiko Aset Kritis

Terdapat 73 risiko dengan nilai RPN tertinggi pada aset dengan nomer ID risiko HW06 dan nilai RPN terendah pada nomer ID risiko HW50.

f. Perangkingan Risiko



Gambar 6. Perangkingan Risiko

Hasil yang diperoleh berdasarkan hasil penilaian adalah terdapat 4 risiko dengan level very high, 8 risiko dengan level high, 14 risiko dengan level medium, 25 risiko dengan level low dan 22 risiko dengan level very low.

g. Mitigasi Risiko

Berdasarkan hasil penilaian dan perangkingan risiko yang dilakukan dengan metode FMEA, maka jumlah dari hasil mitigasi risiko yang dilakukan yaitu :

Tabel 3. Hasil Mitigasi Risiko

Mitigasi	Jumlah
Transferred	9
Limitation	33
Acceptance	5
Avoidance	26

h. Pedoman Kontrol ISO 27002:2013

Hasil mitigasi risiko berdasarkan panduan menggunakan kontrol ISO 27002:2013 pada risiko yang memiliki level risiko *very high* dan *high* yaitu menggunakan klausul 5, klausul 6, klausul 7, klausul 9, klausul 11, klausul 12, klausul 14.

4. KESIMPULAN

Berdasarkan hasil penelitiian terkait analisa dan mitigasi risiko aset kritis terhadap kegagalan proses produksi penyiaran yang dilakukan di TVKU Semarang diperoleh kesimpulan sebagai berikut :

1. Berdasarkan proses identifikasi risiko aset kritis pada TVKU Semarang, diperoleh 73 risiko dimana 56 risiko pada *hardware*, 4 risiko pada *software*, 2 risiko pada *network*, 3 risiko pada *people*, 6 risiko pada data dan 2 risiko pada *procedure*.
2. Berdasarkan hasil identifikasi risiko aset kritis yang mendukung proses produksi penyiaran di TVKU Semarang terdapat beberapa penyebab yang dapat mengganggu dan menghambat proses bisnis penyiaran yang berjalan. Namun penyebab yang paling sering terjadi dan sangat berisiko dapat mengakibatkan proses penyiaran berhenti yaitu risiko pada *server n-computing* dan *server streaming* (*virtual*) yang mengalami *overheat* sampai kurangnya proses *controlling* dan *maintenance*, pada data yang diakibatkan karena *server down*, kabel video rusak, *software hang* yang dikarenakan adanya virus, penyalahgunaan hak akses, dan SOP yang tidak berjalan *efektif*.

3. Berdasarkan penilaian risiko yang dilakukan dengan menggunakan metode FMEA menghasilkan nilai RPN yang diperoleh dari hasil perkalian 3 variabel yaitu *Severity*, *Occurence* dan *Detection*. Hasil dari nilai RPN akan diperoleh berdasarkan level risiko mulai dari *Very High, High, Medium, Low* dan *Very Low*. Hasil perangkingan risiko yang sudah diperoleh yaitu 4 risiko *Very High*, 8 risiko *high*, 14 risiko *medium*, 25 risiko *low* dan 22 risiko *very low*.
4. Berdasarkan hasil penilaian dan perangkingan risiko yang dilakukan dengan metode FMEA, maka jumlah dari hasil mitigasi risiko yang dilakukan adalah *Transferred* = 9, *Limitation* = 33, *Acceptance* = 5 dan *Avoidance* = 26
5. Hasil mitigasi risiko berdasarkan panduan menggunakan kontrol ISO 27002:2013 pada risiko yang memiliki level risiko *very high* dan *high* yaitu menggunakan klausul 5, klausul 6, klausul 7, klausul 9, klausul 11, klausul 12 dan klausul 14.

5. SARAN

Saran yang dapat diberikan oleh penulis untuk perbaikan penelitian tugas akhir berikutnya yaitu:

1. Untuk membantu dalam pembentukan pedoman pelaksanaan kontrol keamanan informasi atas masing-masing penyebab risiko di sarankan menggunakan standar ISO yang lain atau yang terbaru agar lebih bervariasi dalam penanganannya.
2. Setelah dilakukan pencegahan dengan memberikan langkah mitigasi risiko pada hasil identifikasi risiko dan penilaian risiko aset kritis yang terjadi diharapkan untuk penelitian selanjutnya mampu menurunkan jumlah risiko dan level risiko yang terjadi.
3. Untuk penelitian selanjutnya disarankan untuk mendapatkan data dengan menyebarkan kuisioner pada masing-masing karyawan per divisi agar mendapatkan data aset lebih lengkap dan risiko-risiko yang terjadi pada maisng-masing aset dapat lebih detail sehingga dapat lebih meminimalisir risiko tersebut.
4. Melakukan penelitian mitigasi risiko terhadap sistem informasi di suatu perusahaan karena risiko terjadi bukan pada aset kritis saja namun bisa pada sistem informasinya.

DAFTAR PUSTAKA

[1] R. Budiarto, “Penerapan Metode FMEA Untuk Keamanan Sistem Informasi (Studi Kasus : Website POLRI),” pp. 15–17, 2017.

[2] Y. K. Gunawan Setyadi, “Mitigasi Rrisiko Aset dan Komponan Teknologi Informasi berdasarkan kerangka kerja OCTAVE dan FMEA pada Universitas Dian Nuswantoro.”

[3] M. Muslich, *Manajemen Risiko Operasional, Teori dan Praktik*. Bumi Aksara, 2007.

[4] F. R. Destrianto, M. Armys, and R. Sitorus, “Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE,” vol. 9, no. 1, pp. 35–47, 2017.

[5] R. Budiarto, “Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA dan ISO 27001 pada Organisasi XYZ,” vol. 2, no. 2, pp. 48–58, 2017.

[6] D. Anjani, A. P. Subriadi, M. T. A. Hediyanti, S. Kom, and M. Sc, “Identifikasi , Penilaian , dan Mitigasi risiko keamanan informasi pada sistem Electronic Medical Record (Studi kasus : Aplikasi Healthy Plus Modul Rekam Medis di RSU Haji Surabaya).”