ANALISIS DAN PENGUKURAN TINGKAT EKSPOSUR RESIKO TEKNOLOGI INFORMASI DENGAN METODE FMEA PADAPT. BANK CENTRAL ASIA, TBK

Roy Kurniawan

Information Systems Department, School of Information Systems, Binus University
Jl. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
roy_kurniawan@binus.ac.id

ABSTRACT

The purpose of this paper is to help the PT. Bank Central Asia, Tbk in measuring the level of risk exposure and identify the need to control IT risk management at PT. Bank Central Asia, Tbk. Conducted research methodology, field observation, library research, interviews and gave questionnaires to the relevant parties, perform data analysis, as well as measuring the risk of using the approach of FMEA (Failure Mode and Effect Analysis). The results achieved in this study is to facilitate the management in making decisions related to the design, maintenance, and development of information technology at PT. Bank Central Asia, Tbk and also minimize the risk of the failure so that the utilization of existing information technology can provide more optimal results. The conclusion from this study is that there is a risk of potential failure that could hamper the existing business processes in PT. Bank Central Asia, Tbk. Highest risk or potential failure according to the RPN (Risk Priority Number) is a software and hardware damage, as well as the corrupted database due to the impact of operational risk.

Keywords: *risk measurement, information technology, FMEA (Failure Mode and Effect Analysis)*

ABSTRAK

Tujuan penulisan makalah ini adalah untuk membantu PT. Bank Central Asia, tbk dalam mengukur tingkat eksposur resiko serta mengidentifikasi kebutuhan pengendalian untuk penanggulangan resiko IT pada PT. Bank Central Asia, tbk. Metodologi penelitian yang dilakukan, adalah observasi lapangan, studi pustaka, wawancara dan memberikan kuesioner kepada pihak yang terkait, melakukan analisis data, serta melakukan pengukuran resiko menggunakan pendekatan FMEA (Failure Mode and Effect Analysis). Hasil yang dicapai dalam penelitian ini adalah mempermudah pihak manajemen dalam membuat keputusan yang berhubungan dengan perencanaan, pemeliharaan, dan pengembangan teknologi informasi pada PT. Bank Central Asia, tbk dan juga meminimalisir resiko penyebab kegagalan sehingga pemanfaatan teknologi informasi yang ada dapat memberikan hasil yang lebih optimal. Kesimpulan yang didapat dari penelitian ini adalah terdapat resiko kegagalan potensial yang dapat menghambat proses bisnis yang ada di PT. Bank Central Asia, tbk. Resiko atau potensi kegagalan tertinggi menurut RPN (Risk Priority Number) adalah kerusakan software dan hardware, serta database corrupt akibat dampak dari terjadinya resiko operasional.

Kata kunci: *pengukuran, resiko, teknologi informasi, FMEA*

PENDAHULUAN

Menurut Priandoyo (2006), pengukuran atau *assessment* adalah hal yang mutlak dilakukan untuk mendapatkan peningkatan kualitas. Suatu perusahaan dapat meningkatkan penjualan bila mengetahui bagaimana tingkat efisiensi penjualannya. Dengan pengukuran maka perusahaan dapat mengetahui kelemahan yang ada, membandingkan dengan contoh penerapan di perusahaan lain sehingga terdapat peningkatan keuntungan perusahaan. Pada dunia bisnis resiko-resiko bisnis tentu tidak dapat dihindari bagi perusahaan khususnya manajemen resiko walaupun beberapa perusahaan telah melakukan pengelolaan resiko dengan berbagai tingkat kesuksesan. Penerapan manajemen resiko dilakukan secara bertahap dan dijalankan sedini mungkin. Pengimplementasiannya akan berpengaruh pada peningkatan daya saing, flesibilitas, dan pemanfaatan peluang bisnis baru.

Berdasarkan resiko yang diungkap Masing (2009), dikatakan bahwa dengan menggunakan sistem dengan metode manajemen resiko teknologi informasi yang tepat, dapat memiliki pengaruh yang positif bagi perusahaan yaitu dapat mengetahui resiko dan kerentanan, dan dapat mengurangi biaya yang dikeluarkan jika resiko terjadi. PT. Bank Central Asia, tbk merupakan salah satu perusahaan yang telah memanfaatkan teknologi informasi untuk mendukung kegiatan bisnis pada perusahaan agar lebih unggul dan dapat bersaing dari para kompetitornya. Dalam hal ini, pihak manajemen PT. Bank Central Asia, tbk belum pernah melakukan pengukuran resiko terhadap teknologi informasi yang telah diterapkan. Dengan demikian, PT. Bank Central Asia, tbk belum mengetahui sebesar apa resiko yang dapat ditimbulkan dari teknologi informasi yang telah diterapkan dan cara menanggulangi resiko tersebut.

Dalam penulisan ini, penulis menggunakan metode FMEA (*Failure Mode and Effect Analysis*). Karena metode FMEA adalah pendekatan sistematik yang menerapkan suatu metode pentabelan untuk membantu proses pemikiran yang digunakan oleh perusahaan untuk mengidentifikasi mode kegagalan potensial dan efeknya dan untuk mengidentifikasi sumber sumber dan akar penyebab dari suatu masalah kualitas dalam sebuah sistem, desain, proses atau pelayanan pada perusahaan. Oleh karena itu, metode FMEA lebih cocok untuk PT. Bank Central Asia, tbk karena PT. Bank Central Asia, tbk bergerak dibidang perbankan

Masalah yang dibahas dalam penelitian ini adalah: (1) Pengukuran tingkat resiko dan dampak teknologi informasi dengan menggunakan metode FMEA pada PT. Bank Central Asia, tbk. (2) Identifikasi kegagalan potensial, efek kegagalan potensial, rating keparahan (*severity*), penyebab kegagalan potensial, rating kejadian (*occurrence*), evaluasi atau kontrol yang ada, metode deteksi (*detection*) dan RPN (*Risk Priority Number*) pada PT. Bank Central Asia, tbk. (3) Identifikasi metode mitigasi untuk mengontrol dan penanggulangan resiko pada PT. Bank Central Asia, tbk

Untuk lebih mengarahkan penyusunan dan penulisan, ruang lingkup penelitian dibatasi pada: (1) Penelitian dilakukan pada PT. Bank Central Asia, tbk. (2) Penelitian dilakukan pada divisi IT PT. Bank Central Asia, tbk. (3) Pengukuran resiko teknologi informasi pada PT. Bank Central Asia, tbk menggunakan pendekatan metode FMEA (*Failure Mode and Effect Analysis*).

Tujuan yang ingin dicapai adalah: (1) Mengidentifikasi resiko teknologi informasi serta dampaknya pada PT. Bank Central Asia, tbk. (2) Mengkuantifikasi tingkat resiko dan dampak teknologi informasi dengan menggunakan metode FMEA pada PT. Bank Central Asia, tbk. (3) Mengukur resiko teknologi informasi dan dampak resiko berdasarkan identifikasi mode kegagalan potensial, efek kegagalan potensial, rating keparahan (*severity*), penyebab kegagalan potensial, rating kejadian (*occurrence*), evaluasi atau kontrol yang ada, metode deteksi (*detection*) dan RPN (*Risk Priority Number*) pada PT. Bank Central Asia, tbk. (4) Mengidentifikasi prioritas, metode mitigasi, kebutuhan pengendalian untuk penanggulangan resiko IT pada PT. Bank Central Asia, tbk. (5) Meminimalisir kerugian yang disebabkan kegagalan potensial akibat resiko IT dan efeknya.

Manfaat yang ingin dicapai dalam penulisan ini adalah: (1) Meminimalkan resiko atau mode kegagalan potensial, efek kegagalan potensial dan penyebab kegagalan yang ada pada PT. Bank Central Asia, tbk . (2) Meminimalkan resiko terjadinya ancaman yang datang dari dalam maupun dari luar perusahaan. (3) Memberikan kemudahan kepada pihak manajemen PT. Bank Central Asia, tbk untuk menangani resiko-resiko atau mode kegagalan potensial, efek kegagalan potensial dan penyebab kegagalan yang ditemukan dari hasil penelitian. (4) Memberikan pengetahuan tentang pengukuran resiko teknologi informasi terhadap perusahaan. (5) Sebagai referensi untuk peneliti selanjutnya.

METODE

Teknik Pengumpulan Data

Penelitian Lapangan (Field Research)

Penelitian lapangan merupakan penelitian kualitatif di mana peneliti mengamati dan berpartisipasi secara langsung dalam penelitian skala sosial kecil dan mengamati budaya setempat dengan cara mengunjungi perusahaan, data didapatkan dengan cara-cara: (1) Observasi. Observasi adalah bagian dalam pengumpulan data yang berarti mengumpulkan data langsung dari lapangan. Data dikumpulkan dari log pada sistem internal dan beberapa core application serta data dari divisi terkait yaitu Divisi IT, manajemen resiko dan keuangan. (2) Wawancara. Wawancara adalah sebuah dialog yang dilakukan oleh pewawancara untuk memperoleh informasi dari terwawancara. Wawancara dilakukan terhadap beberapa karyawan divisi IT sejumlah 15 orang dari beberapa 8 biro yang berbeda. (3) Kuesioner. Kuesioner merupakan teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawabnya. Kuesioner berupa 8 pertanyaan dengan 4 - 5 point dibagikan kepada seluruh karyawan divisi IT sejumlah 75 karyawan tetap, 82 karyawan kontrak dan 25 karyawan outsource. Total kuesioner berjumlah 182.

Penelitian Kepustakaan (Library Research)

Studi kepustakaan merupakan langkah yang penting dimana setelah seorang peneliti menetapkan topik penelitian.

Teknik Analisis

Pengukuran resiko teknologi informasi pada PT. Bank Central Asia, tbk menggunakan pendekatan teknik analisa FMEA (*Failure Mode and Effect Analysis*) dengan menyajikan secara rinci langkah-langkah untuk mengukur tingkat resiko yang ada di perusahaan yang bergerak di bidangperbankan

Metode FMEA (*Failure Mode and Effect Analysis*)

Menurut Keskin (2008). "*Mode and Effects Analysis (FMEA) is a technique used to improve productivity. It is a method that evaluates possible failures in the system, design, process or service. It aims to continuously improve and decrease these kinds of failure modes"*. FMEA adalah teknik yang digunakan untuk meningkatkan produktivitas. Ini adalah metode yang mengevaluasi kemungkinan kegagalan dalam proses, desain, sistem atau layanan. Menurut The International Marine Contractor Association (IMCA) (2002), "FMEA *is design tool that has been around for many years and is recognized as an essential function in design from concept through to the development of every conceivable type of equipment"*. FMEA adalah alat desain yang telah ada selama bertahun-tahun dan diakui sebagai fungsi penting dalam desain, dari konsep hingga pengembangan di setiap jenis peralatan.

Terdapat lima tipe FMEA yang bisa diterapkan, yaitu: (1) *System*, digunakan untuk menganalisa sistem dan subsistem pada konsep pemulaan dan tahap desain. Fokus pada jenis-jenis kegagalan produk yang berhubungan dengan fungsi sebuah sistem yang diakibatkan oleh defisiensi desain. Termasuk interaksi sebuah sistem dengan sistem lainnya, dan interaksi antar elemen-elemen sistem. (2) *Design*, digunakan untuk menganalisa produk. Fokus pada jenis-jenis kegagalan pada suatu produk yang diakibatkan oleh defisiensi desain. (3) *Process*, digunakan untuk menganalisa proses. Fokus pada jenis-jenis kegagalan potensial yang diakibatkan oleh defisiensi desain proses. (4) *Service*, berfokus pada fungsi jasa. (5) *Software*, berfokus pada fungsi *software.*

Tahapan FMEA adalah sebagai berikut: (1) Deskripsi/tujuan. (2) Identifikasi kegagalan potensial. (3) Identifikasi efek kegagalan potensial. (4) Menentukan *severity* atau *rating* keparahan. (5) Penyebab kegagalan potensial. (6) Menentukan *occurrence* atau *rating* kejadian. (7) Evaluasi atau *control yang ada.* (8) Identifikasi metode deteksi. (9) Menghitung RPN (*Risk Priority Number*). (10) Rekomendasi

Manfaat FMEA

Dari penerapan FMEA pada perusahaan, maka akan dapat diperoleh keuntungan-keuntungan yang sangat bermanfaat untuk perusahaan, antara lain: (1) Meningkatkan kualitas, keandalan, dan keamanan produk. (2) Membantu meningkatkan kepuasan pelanggan. (3) Meningkatkan citra baik dan daya saing perusahaan. (4) Mengurangi waktu dan biaya pengembangan produk. (5) Memperkirakan tindakan dan dokumen yang dapat menguangi resiko.

Pengukuran resiko yang dilakukan pada divisi IT PT. Bank Central Asia, tbk dilakukan dengan mengumpulkan dan mengolah data berdasarkan wawancara dan kuesioner yang telah dibagikan kepada divisi IT di PT. Bank Central Asia, tbk . Kuesioner yang dibagikan digunakan untuk mengetahui kelemahan dari hasil pengukuran resiko serta mencari solusi atas resiko-resiko yang terjadi di divisi IT PT. Bank Central Asia, tbk .

HASIL DAN PEMBAHASAN

Analisa FMEA PT. Bank Central Asia, tbk

Pada PT. Bank Central Asia, tbk terdapat beberapa potensi kegagalan yang ada, yaitu *software server* rusak atau *error*, *hardware server* rusak, *memory server full*, data atau *file corrupt, database corrupt*, *scan barcode* rusak/tidak berfungsi dengan baik, komputer *client* rusak, komputer *client* melambat kinerjanya, dan LAN rusak/tidak berfungsi dengan baik. Dari beberapa potensi kegagalan yang ada di perusahaan, ada akibat yang ditimbulkan dari potensi kegagalan tersebut yang dapat membuat proses bisnis yang ada diperusahaan menjadi terganggu, bahkan dapat menyebabkan kerugian bagi perusahaan. Oleh karena itu, peneliti melakukan pengukuran resiko menggunakan metode FMEA (*Failure Mode and Effect Analysis*) untuk memberi informasi kepada perusahaan dalam menangani dan mengatasi resiko yang ada di perusahaan.

Software Server Error

Software server error dapat mengakibatkan *server* tidak bisa mengendalikan seluruh komputer yang ada di perusahaan. Sesuai dari kuesioner, *severity* atau *rating* keparahan dari *software server* rusak atau *error* ini terdapat di angka 10, yaitu akibat yang ditimbulkan sangat berbahaya bagi perusahaan. Adapun penyebab-penyebab terjadi *software server* rusak yang biasa terjadi di perusahaan sesuai dengan wawancara yang dilakukan dengan pihak divisi IT perusahaan yaitu listrik padam, *human error*, dan virus.

Listrik Padam

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari listrik padam ini terdapat di angka 9 yaitu tergolong *high.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari listrik padam sesuai dari hasil wawancara yaitu perusahaan menyediakan UPS (*Uninteruptable Power System*) dan *server backup*. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 6, yaitu metode pencegahan masih kurang efektif dan penyebab masih berulang kembali. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 540. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan mengadakan control UPS (*Uninteruptable Power System*) secara berkala dan menyediakan generator set atau yang biasa disebut genset di perusahaan demi meminimalisir resiko dari listrik padam tersebut.

Human Error

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 5 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *human error* sesuai dari hasil wawancara yaitu perusahaan memberikan batasan akses. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 4, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 200. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan memberikan bimbingan dan pelatihan SDM (Sumber Daya Manusia) kepada karyawan yang berhubungan dengan sistem informasi.

Virus

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari virus ini terdapat di angka 6 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari virus yaitu antivirus dan jadwal maintenance. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 2, yaitu kemungkinan penyebab resiko terjadi sangat rendah. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 162. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan meng-*update* antivirus secara berkala.

Hardware Server Rusak

Hardware server rusak dapat mengakibatkan server tidak bisa mengendalikan seluruh komputer yang ada di perusahaan. Sesuai dari kuesioner, *severity* atau *rating* keparahan dari *software server* rusak atau *error* ini terdapat di angka 9, yaitu akibat yang ditimbulkan sangat berbahaya bagi perusahaan. Adapun penyebab-penyebab terjadinya *hardware server* rusak yang biasa terjadi di perusahaan sesuai dengan wawancara yang dilakukan dengan pihak divisi IT perusahaan yaitu listrik padam, *hardware* tidak terawat dengan baik dan *human error.*

Listrik Padam

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari listrik padam ini terdapat di angka 6 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari listrik padam sesuai dari hasil wawancara yaitu perusahaan menyediakan UPS (*Uninteruptable Power System*) dan *server backup*. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 6, yaitu metode pencegahan masih kurang efektif dan penyebab masih berulang kembali. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 324. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati

oleh pihak divisi IT perusahaan yaitu dengan mengadakan control UPS (*Uninteruptable Power System*) secara berkala dan menyediakan *generator set* atau yang biasa disebut *genset* di perusahaan demi meminimalisir resiko dari listrik padam tersebut.

***Hardware* Tidak Terawat**

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *hardware* tidak terawat dengan baik ini terdapat di angka 4 yaitu tergolong *low*. Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *hardware* tidak terawat dengan baik sesuai dari hasil wawancara yaitu jadwal *maintenance*. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 1, yaitu kemungkinan penyebab resiko sangat rendah. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 36. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu *maintenance* secara berkala dan membuat kebijakan peremajaan hardware yang sudah tidak layak pakai.

Human Error

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 2 yaitu tergolong *low*. Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *human error* sesuai dari hasil wawancara yaitu perusahaan memberikan batasan akses. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 5, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 90. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan memberikan bimbingan dan pelatihan SDM (Sumber Daya Manusia) kepada karyawan yang berhubungan dengan sistem informasi.

Memory Server Full

Memory Server Full mengakibatkan *server* tidak dapat menyimpan data yang ada dan komputer menjadi lambat kinerjanya/lemot. Sesuai dari kuesioner, *severity* atau *rating* keparahan dari *memory server full* ini terdapat di angka 4, yaitu *moderate severity* (pengaruh buruk yang moderat). Pengguna akan merasakan penurunan kinerja, namun masih dalam batas toleransi. Adapun penyebab-penyebab terjadinya *memory server full* yang biasa terjadi di perusahaan sesuai dengan wawancara yang dilakukan dengan pihak divisi IT perusahaan yaitu *worm*, *file* ganda/duplikat, *file* tidak penting (foto, video, lagu, dll), dan *human error*.

Worm

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *worm* ini terdapat di angka 4 yaitu tergolong *low*. Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari worm sesuai dari hasil wawancara yaitu antivirus dan jadwal *maintenance*. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 4, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 64. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu menggunakan antivirus yang asli dan update antivirus secara berkala.

File Ganda/Duplikat

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *file* ganda/duplikat ini terdapat di angka 8 yaitu tergolong *high.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *file* ganda/duplikatsesuai dari hasil wawancara yaitu pemeriksaaan

dan sosialisasi peraturan. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 5, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 160. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu pemeriksaaan dan sosialiasi peraturan secara berkala.

File Tidak Penting

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari file tidak penting ini terdapat di angka 9 yaitu tergolong *high.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *file* ganda/duplikat sesuai dari hasil wawancara yaitu pemeriksaaan dan sosialisasi peraturan. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 6, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 216. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu membuat *permission folder*.

Human Error

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 4 yaitu tergolong *low*. Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *human error* sesuai dari hasil wawancara yaitu perusahaan memberikan kuota penyimpanan. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 6, yaitu metode pencegahan masih kurang efektif dan penyebab masih berulang kembali. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 96. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan menambah kapasitas memory.

Database Corrupt

Database Corrupt mengakibatkan *server* atau *user* tidak dapat mengetahui data atau informasi yang ada dalam *database*. Sesuai dari kuesioner, *severity* atau *rating* keparahan dari *database corrupt* ini terdapat di angka 9, yaitu *high severity* (pengaruh buruk yang tinggi). Pengguna akan merasakan akibat buruk yang tidak akan diterima, berada di luar batas toleransi. Adapun penyebab-penyebab terjadinya database corrupt yang biasa terjadi di perusahaan sesuai dengan wawancara yang dilakukan dengan pihak divisi IT perusahaan yaitu listrik padam, virus, dan *human error*.

Listrik Padam

Sesuai dari hasil kuesioner yang diberikan *rating* kejadian atau *occurrence* dari listrik padam ini terdapat di angka 9 yaitu tergolong *high.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari listrik padam sesuai dari hasil wawancara yaitu perusahaan menyediakan UPS (*Uninteruptable Power System*) dan *server backup*. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 6, yaitu metode pencegahan masih kurang efektif dan penyebab masih berulang kembali. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence*, dan *detection* adalah 486. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan mengadakan control UPS (*Uninteruptable Power System*) secara berkala dan menyediakan generator set atau yang biasa disebut genset di perusahaan demi meminimalisir resiko dari listrik padam tersebut.

Virus

Sesuai dari hasil kuesioner yang diberikan *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 5 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk

menanggulangi resiko dari virus yaitu antivirus dan jadwal *maintenance.* Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 2, yaitu kemungkinan penyebab resiko terjadi sangat rendah. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 90. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan menggunakan antivirus yang asli dan mengupdate antivirus secara berkala.

Human Error

Sesuai dari hasil kuesioner yang diberikan *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 3 yaitu tergolong *low.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *human error* sesuai dari hasil wawancara yaitu *backup* data. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 5, yaitu metode pencegahan masih kurang efektif dan penyebab masih berulang kembali. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 135. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan memberikan bimbingan dan pelatihan SDM (Sumber Daya Manusia) kepada karyawan yang berhubungan dengan sistem informasi.

Data Diketahui oleh Orang yang Tidak Berwenang

Data diketahui oleh orang yang tidak mempunyai wewenang mengakibatkan informasi yang ada disalahgunakan oleh orang yang tidak mempunyai wewenang tersebut dan berakibat kerugian bagi perusahaan. Sesuai dari kuesioner, *severity* atau *rating* keparahan dari data diketahui oleh orang yang tidak mempunyai wewenang ini terdapat di angka 8, yaitu *high severity* (pengaruh buruk yang tinggi). Pengguna akan merasakan akibat buruk yang tidak akan diterima, berada di luar batas toleransi. Adapun penyebab-penyebab terjadinya data diketahui oleh orang yang tidak mempunyai wewenang yang biasa terjadi di perusahaan sesuai dengan wawancara yang dilakukan dengan pihak divisi IT perusahaan yaitu memberikan dan memberitahu *password* kepada orang lain yang tidak berwenang, lupa *logout, human error,* dan *hacker* atau *cracker* dari orang dalam di perusahaan.

Memberikan dan Memberitahu *Password* kepada Orang Lain

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari memberikan dan memberitahu *password* kepada orang lain yang tidak berwenang ini terdapat di angka 9 yaitu tergolong *high.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari memberikan dan memberitahu *password* kepada orang lain yang tidak berwenang sesuai dari hasil wawancara yaitu pemeriksaan, sosialisasi peraturan dan sanksi. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 4, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 288. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan me-*reset password* secara berkala.

Lupa Logout

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari lupa *logout* ini terdapat di angka 7 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari lupa *logout* sesuai dari hasil wawancara yaitu teguran. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 5, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 280. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu menggunakan sistem otomatis *sleep*.

Human Error

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 5 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *human error* sesuai dari hasil wawancara yaitu sanksi indisipliner. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 5, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 200. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan memberikan bimbingan dan pelatihan SDM (Sumber Daya Manusia).

Komputer *Client* Rusak

Komputer *client* rusak mengakibatkan karyawan atau staff tidak dapat bekerja sebagaimana mestinya. Sesuai dari kuesioner, *severity* atau rating keparahan dari komputer client rusak ini terdapat di angka 2, yaitu *mild severity.* Akibat yang ditimbulkan hanya bersifat ringan bagi perusahaan. Adapun penyebab-penyebab terjadinya komputer client rusak yang biasa terjadi di perusahaan sesuai dengan wawancara yang dilakukan dengan pihak divisi IT perusahaan yaitu listrik padam, virus, dan *human error*.

Listrik Padam

Sesuai dari hasil kuesioner yang diberikan, rating kejadian atau *occurrence* dari listrik padam ini terdapat di angka 7 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari listrik padam sesuai dari hasil wawancara yaitu perusahaan menyediakan UPS (*Uninteruptable Power System*) dan server backup. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 5, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 70. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan mengadakan control UPS (*Uninteruptable Power System*) secara berkala dan menyediakan generator set atau yang biasa disebut *genset* di perusahaan demi meminimalisir resiko dari listrik padam tersebut.

Virus

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari virus ini terdapat di angka 7 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari virus yaitu antivirus dan jadwal *maintenance*. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 2, yaitu kemungkinan penyebab resiko terjadi sangat rendah. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 28. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan menggunakan antivirus asli dan meng-*update* antivirus secara berkala.

Human Error

Sesuai dari hasil kuesioner yang diberikan, rating kejadian atau *occurrence* dari *human error* ini terdapat di angka 6 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *human error* sesuai dari hasil wawancara yaitu perusahaan memberikan teguran sampai sanksi. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 4, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 48. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu

dengan memberikan bimbingan dan pelatihan SDM (Sumber Daya Manusia) kepada karyawan yang berhubungan dengan sistem informasi.

Komputer *Client* Melambat Kinerja

Komputer *client* melambat kinerjanya mengakibatkan pekerjaan yang dilakukan menjadi terhambat. Sesuai dari kuesioner, *severity* atau *rating* keparahan dari komputer *client* rusak ini terdapat di angka 1, yaitu *mild severity.* Akibat yang ditimbulkan hanya bersifat ringan bagi perusahaan. Adapun penyebab-penyebab terjadinya komputer *client* rusak yang biasa terjadi di perusahaan sesuai dengan wawancara yang dilakukan dengan pihak divisi IT perusahaan yaitu memory penuh / *full, worm*, virus, *human error*.

Memory Server Full

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari memory full ini terdapat di angka 8 yaitu tergolong *high.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari memory fullsesuai dari hasil wawancara yaitu jadwal *maintenance*. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 5, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 40. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu membuat *system backup* otomatis.

Worm

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *worm* ini terdapat di angka 5 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *worm* sesuai dari hasil wawancara yaitu antivirus dan jadwal maintenance. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 2, yaitu metode memungkinkan penyebab itu terjadi sangat rendah. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 10. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu menggunakan antivirus yang asli dan meng-*update* antivirus secara berkala.

Virus

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 7 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari virus yaitu antivirus dan jadwal *maintenance*. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 3, yaitu kemungkinan penyebab resiko terjadi sangat rendah. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 21. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan menggunakan antivirus yang asli dan meng-*update* antivirus secara berkala.

Human Error

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 4 yaitu tergolong *low.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *human error* sesuai dari hasil wawancara yaitu memberi teguran. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 5, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 20. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan memberikan bimbingan dan

pelatihan SDM (Sumber Daya Manusia) kepada karyawan yang berhubungan dengan sistem informasi.

LAN Rusak atau Tidak Berfungsi dengan Baik

LAN rusak atau tidak berfungsi dengan baik kinerjanya dapat mengakibatkan komputer server /client tidak dapat berhubungan satu sama lain dalam proses terima/ mengirim data. Sesuai dari kuesioner, *severity* atau rating keparahan dari computer computer klien rusak ini terdapat di angka 8, yaitu *high severity* (pengaruh buruk yang tinggi). Pengguna akan merasakan akibat buruk yang tidak akan diterima, berada di luar batas toleransi. Adapun penyebab-penyebab terjadinya database corrupt yang biasa terjadi di perusahaan sesuai dengan wawancara yang dilakukan dengan pihak divisi IT perusahaan yaitu Kabel / peralatan LAN rusak, dan human error.

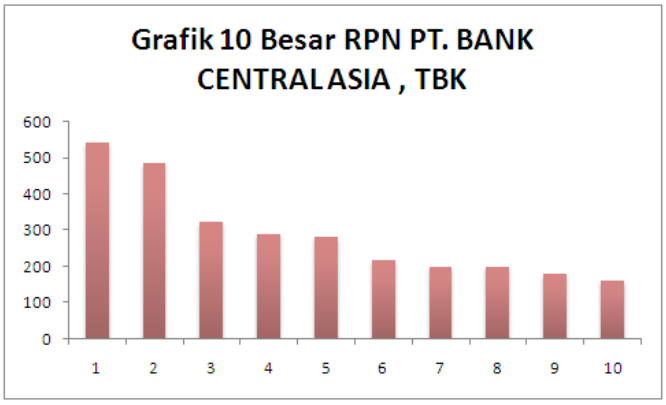
Kabel / Peralatan LAN Rusak

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 7 yaitu tergolong *high.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari kabel atau peralatan LAN rusaksesuai dari hasil wawancara yaitu jadwal cek peralatan dan perbaikan. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 2, yaitu kemungkinan penyebab resiko terjadi sangat rendah. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 112. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu Pemeriksaan secara berkala.

Human Error

Sesuai dari hasil kuesioner yang diberikan, *rating* kejadian atau *occurrence* dari *human error* ini terdapat di angka 4 yaitu tergolong *moderate.* Metode evaluasi yang ada di perusahaan untuk menanggulangi resiko dari *human error* sesuai dari hasil wawancara yaitu memberi teguran sampai sanksi. Nilai *detection* atau kemampuan mendeteksi resiko sesuai dari kuesioner terdapat di angka 5, yaitu metode pencegahan kadang memungkinkan penyebab itu terjadi. Nilai RPN yang dihasilkan dari perkalian *severity, occurrence,* dan *detection* adalah 160. Rekomendasi yang diberikan sesuai dengan hasil diskusi dan telah disepakati oleh pihak divisi IT perusahaan yaitu dengan memberikan bimbingan dan pelatihan SDM (Sumber Daya Manusia) kepada karyawan yang berhubungan dengan sistem informasi.

Tabel dan Grafik RPN (Risk Priority Number)



Gambar 1 Grafik 10 besar RPN PT. Bank Central Asia, tbk

Tabel 1 RPN PT. Bank Central Asia, tbk

Prioritas	Potensi Kegagalan	Penyebab potensi kegagalan	Severity	Occurrence	Detection	RPN
1	Software server error	Listrik padam	10	9	6	540
2	Database corrupt	Listrik padam	9	9	6	486
3	Hardware server rusak	Listrikpadam	9	6	6	324
4	Data diketahui pihak tidak mempunyai wewenang	Memberitahu password	8	9	4	288
5	Data diketahui pihak tidak mempunyai wewenang	Lupa Logout	8	7	5	280
6	Memory server full	File tidak penting	4	9	6	216
7	Data diketahui pihak tidak mempunyai wewenang	*Human Eror*	8	5	5	200
8	Software server error	*Human Eror*	10	5	4	200
9	Software server error	*Worm*	10	6	3	180
10	Memory server full	File ganda/duplikat	4	8	5	160
11	LAN rusak	*Human Eror*	8	4	5	160
12	Database corrupt	*Human Error*	9	3	5	135
13	Software server error	Virus	10	6	2	120
14	LAN rusak	Peralatan LAN rusak sesuai	8	7	2	112
15	Memory server full	*Human Error*	4	4	6	96
16	Hardware server rusak	*Human Eror*	9	2	5	90
17	Database corrupt	Virus	9	5	2	90
18	Komputer client rusak	Listrik padam	2	7	5	70
19	Memory server full	*Worm*	4	4	4	64
20	Komputer client rusak	*Human Error*	2	6	4	48
21	Komputer client melambat kinerjanya	Memory server full	1	8	5	40
22	Hardware server rusak	Hardware tidak terawat	9	4	1	36
23	Komputer client rusak	Virus	2	7	2	28
24	Komputer client melambat kinerjanya	Virus	1	7	3	21
25	Komputer client melambat kinerjanya	*Human Eror*	1	4	5	20
26	Komputer client melambat kinerjanya	*Worm*	1	5	2	10

Tabel 2 10 Besar RPN PT. Bank Central Asia, tbk

Prioritas	Potensi Kegagalan	Penyebab potensi kegagalan	RPN
1	Software server error	Listrik padam	540
2	Database corrupt	Listrik padam	486
3	Hardware server rusak	Listrikpadam	324
4	Data diketahui pihak tidak mempunyai wewenang	Memberitahu password	288
5	Data diketahui pihak tidak mempunyai wewenang	Lupa Logout	280
6	Memory server full	File tidak penting	216
7	Data diketahui pihak tidak mempunyai wewenang	*Human Eror*	200
7	Software server error	*Human Eror*	200
9	Software server error	*Worm*	180
10	Memory server full	File ganda/duplikat	160
10	LAN rusak	*Human Eror*	160

SIMPULAN

Berdasarkan hasil penelitian pengukuran resiko yang dilakukan pada divisi IT PT. Bank Central Asia, tbk dapat disimpulkan: (1) Terdapat beberapa resiko yang menyebabkan kerugian potensial dan menghambat proses bisnis. Potensi penyebab kegagalan potensial terbesar yaitu *hardware server* yang rusak, *database corrupt* dan *software server* rusak atau *error*. Ketika *software* maupun *hardware server* dan *database* tidak berfungsi optimal, maka berbagai proses bisnis serta jalannya operasional akan terganggu dan menjadi tidak optimal. (2) Adanya potensi penyebab dari kegagalan yang ada pada PT. Bank Central Asia, tbk, dan tingkat tertinggi dari penyebab kegagalan tersebut adalah pada saat listrik mengalami pemadaman (baik karena kerusakan teknis maupun non teknis) oleh pihak PLN (Perusahaan Listrik Negara) yang mengakibatkan perusahaan tidak mendapat pasokan listrik. (3) Adanya potensi penyebab kegagalan yang ada pada PT. Bank Central Asia, tbk yaitu memberikan dan memberitahu password kepada orang yang tidak mempunyai wewenang yang dapat meyebabkan informasi perusahaan dapat disalahgunakan dan dapat berdampak kerugian bagi perusahaan. (4) Adanya potensi penyebab kegagalan yang ada di PT. Bank Central Asia, tbk yang terdapat dibeberapa potensi kegagalan yaitu *human error* yang berdampak buruk bagi perusahaan dan dapat mengakibatkan kerugian bagi perusahaan. (5) Terdapat potensi kegagalan yang ada di PT. Bank Central Asia, tbk yaitu data yang ada di perusahaan diketahui oleh orang yang tidak mempunyai wewenang yang dapat mengakibatkan informasi tentang perusahaan atau informasi yang ada diperusahaan disalahgunakan oleh orang yang tidak mempunyai wewenang tersebut dan dapat berdampak kerugian bagi perusahaan. (6) Pengukuran resiko tekhnologi informasi sangat diperlukan bagi PT. Bank Central Asia, tbk untuk meminimalisir resiko yang sering terjadi di perusahaan yang dapat mengakibatkan kerugian bagi perusahaan.

Berdasarkan hasil penelitian manajemen resiko yang dilakukan pada divisi IT PT. Bank Central Asia, tbk dapat disarankan: (1) Demi memitigasi kerusakan *hardware* yang mengakibatkan operasional tidak berjalan optimal, disarankan untuk melakukan pengecekan *hardware* secara berkala, dan selalu membackup data-data yang penting minimal setiap hari sekali. (2) Untuk memitigasi pemadaman listrik perusahaan perlu penambahan dan kontrol secara berkala UPS (*Uninteruptable Power System*) untuk pemadaman yang jangka waktunya lebih sedikit, dan diperlukan general set untuk jangka waktu yang lebih lama serta ada pengecekan secara berkala agar alat berfungsi dengan baik. (3) Untuk meminimalisir terjadinya *human error* yang sering terjadi di perusahaan, PT. Bank Central Asia, tbk disarankan melakukan bimbingan dan pelatihan terhadap SDM (Sumber Daya Manusia) yang berhubungan dengan teknologi informasi atau sistem informasi untuk memberikan wawasan dan pengetahuan tentang tekhnologi atau sistem informasi bagi SDM (Sumber Daya Manusia) yang ada di perusahaan. (4) Untuk memitigasi virus, worm, dan lain-lain yang dapat menyebabkan sistem tidak dapat berfungsi optimal disarankan menggunakan antivirus yang asli disetiap komputer yang ada di perusahaan dan meng-*update* antivirus secara berkala. (5) Untuk meminimalisir terjadinya *user* lupa me-*logout* sistem di perusahaan, disarankan untuk menggunakan sistem otomatis *sleep* di setiap komputer yang ada diperusahaan untuk meminimalisir kerugian yang ditimbulkan oleh *user* yang lupa *logout*.

DAFTAR PUSTAKA

Keskin, G. A., Ozkan, K. (2008). *Quality and Reliability Engineering International: An Alternative Evaluation of FMEA (Fuzzy Art lgorithm).* WileyInterScience.

Masing, E. (2009). Tehnical Support : Improving Performance and Reduing Costs With IT Risk Management. Risk Management. *The International Marine Contractors Asosiation*. *56*(8), 48-51

Priandoyo, A. (2006). Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi. *Jurnal Sistem Informasi*. *1*(2).