TUGAS AKHIR – KS14 1501

KONSISTENSI PENGGUNAAN METODE FMEA TERHADAP PENILAIAN RISIKO TEKNOLOGI INFORMASI (Studi Kasus: Bank XYZ)

Brigitta Devianti Cahyabuana
NRP 5211100011

DosenPembimbing
Dr. ApolPribadi S., S.T, M.T

JURUSAN SISTEM INFORMASI
FakultasTeknologiInformasi
InstitutTeknologiSepuluhNopember
Surabaya 2015

FINAL PROJECT – KS14 1501

CONSISTENCY OF FMEA METHODE FOR ASSESSING INFORMATION TECHNOLOGY RISK (CASE STUDY: XYZ BANK)

Brigitta Devianti Cahyabuana
NRP 5211100011

Supervisor
Dr. ApolPribadi S., S.T, M.T

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Institute of Technology SepuluhNopember
Surabaya 2015

KONSISTENSI PENGGUNAAN METODE FMEA TERHADAP PENILAIAN RISIKO TEKNOLOGI INFORMASI (Studi Kasus : Bank XYZ)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

BRIGITTA DEVIANTI CAHYABUANA
5211 100 011

Surabaya, Januari 2015

KETUA
JURUSAN SISTEM INFORMASI

Dr. Eng. Febriliyan Samopa S.Kom., M.Kom.
NIP 19730219 199802 1 001

KONSISTENSI PENGGUNAAN METODE FMEA TERHADAP PENILAIAN RISIKO TEKNOLOGI INFORMASI (Studi Kasus : Bank XYZ)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :
BRIGITTA DEVIANTI CAHYABUANA
5211 100 011

Disetujui Tim Penguji : Tanggal Ujian : 17 Januari 2015
Periode Wisuda : Maret 2015

Dr. Apol Pribadi S., S.T, M.T **(Pembimbing)**

Sholiq, S.T., M.Kom, M.SA **(Penguji 1)**

Bekti Cahyo Hidayanto, S.Si., M.Kom **(Penguji 2)**

KONSISTENSI PENGGUNAAN METODE FMEA TERHADAP PENILAIAN RISIKO TEKNOLOGI INFORMASI

Nama Mahasiswa : BRIGITTA DEVIANTI CAHYABUANA
NRP : 5211 100 011
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing : Dr. Apol Pribadi S., S.T, M.T

ABSTRAK

Perkembangan teknologi informasi semakin berkembang pesat dan semakin banyak pemanfaatan teknologi informasi diberbagai bidang. Tak terkecuali dalam dunia perbankan, semakin banyak perusahaan perbankan memanfaatkan teknologi informasi untuk mempermudah proses bisnis dan memudahkan para nasabah memiliki berbagai kemudahan. Teknologi informasi yang digunakan berpotensi memiliki risiko sehingga diperlukan analisis manajemen risiko.

Analisis manajemen risiko pada penggunaan teknologi informasi diperlukan suatu metode dalam melakukan pemrioritasan nilai risiko. Metode yang digunakan dalam melakukan pemrioritasan risiko adalah Failure Mode Effect and Analysis (FMEA). Penilaian risiko ini digunakan pada studi kasus penggunaan teknologi informasi pada teller Bank XYZ. Penilaian risiko ini, dilakukan oleh dua tim yang berbeda untuk membandingkan hasil yang diperoleh serta untuk mengetahui apakah penilaian yang dilakukan memiliki hasil yang konsisten atau tidak.

Analisis mengenai konsistensi hasil penilaian risiko menggunakan metode FMEA, dilakukan metode analisis kesenjangan dan metode kualitatif untuk mengidentifikasi penyebab dari hasil penilaian risiko yang tidak sama. Hasil yang didapatkan mengenai penyebab penilaian risiko menggunakan metode FMEA menjadi belum konsisten adalah metode pemrioritasan yang digunakan, prosedur dalam melakukan

penilaian risiko, pengetahuan narasumber, dan kemampuan fasilitator dalam melakukan penilaian risiko menggunakan metode FMEA.

Hasil penilaian risiko menggunakan metode FMEA yang belum konsisten, menjadi acuan dalam membuat kerangka FMEA yang disesuaikan dengan kebutuhan Bank XYZ dalam melakukan penilaian risiko.

Penelitian ini diharapkan menunjukkan hasil dari konsistensi penggunaan metode FMEA dan pembuatan rekomendasi perbaikan penggunaan metode FMEA yang sesuai dengan kondisi perusahaan XYZ.

Kata kunci : *manajemen risiko teknologi informasi, penilaian risiko, pemrioritasan risiko, FMEA, konsistensi metode FMEA*.

CONSISTENCY OF FMEA METHODE FOR ASSESSING INFORMATION TECHNOLOGY RISK

Name : BRIGITTA DEVIANTI CAHYABUANA
NRP : 5211 100 011
Department : Information Systems FTIF -ITS
Supervisor : Dr. Apol Pribadi S., S.T, M.T

Abstract

The development of information technology is growing rapidly. A company as the business actor needs media to give the simple way to run the business process for reaching the maximum profits. Therefore, The implementation of information technology becomes the needs among the business owners for running their business. Nowdays, In Bank sector, the using of information technology uses for supporting the business process

Analysis of risk management on the using of the information technology in company which needs method to priotize the risk. The methode for priotizing the risk, can use Failure Mode Effect and Analysis (FMEA) methode for risk management. The risk assessment of this case study is used the using of information technology in teller of Bank XYZ. The risk assessment was done by two different teams to compare the assessment result which could give the consisten result or not.

Analysis of the consistency of the using of FMEA, used the gap analysis and qualitative methods to identify the cause of the difference result when assess the risk. The resulf of the cause of inconcistency of assess the risk by using FMEA method, are the priotize method used, procedure to assess the risk, the

informarman knowledge, and the ability of the facilitator to guide when assess the risk by using FMEA method.

The inconcistency result of the using FMEA method, is used to be reference for creating the FMEA framework which is addapted with the company needs to assess the risk.

The research is expected to show the result of the consistency of the using FMEA method to assess the risk and give the recommendation for assessing the risk with the need of the company to assess the risk, based on the company condition and need.

Keywords: risk management of information technology, risk assessment, risk priority, FMEA, consistency of FMEA.

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa, karena berkat, kasih sayang, dan tuntunan-Nya untuk memberikan kemudahan dan kelancaran dalam setiap pengerjaain Tugas Akhir yang berjudul:

KONSISTENSI PENGGUNAAN METODE FMEA TERHADAP PENILAIAN RISIKO TEKNOLOGI INFORMASI (STUDI KASUS: BANK XYZ)

yang menjadi salah satu syarat untuk memperoleh gelar sebagai Sarjana Sistem Informasi Strata Satu di Institut Teknologi Sepuluh Nopember.

Tugas Akhir ini dapat selesai dikerjakan berkat dukungan, bimbingan, bantuan, dan doa dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih yang begitu mendalam kepada seluruh pihak yang telah berproses dalam membantu pengerjaan Tugas Akhir ini.

1. Dosen pembimbing, Yang Terhormat Bapak Dr. Apol Pribadi Subriadi, S.T, M.T yang begitu sabar memberikan bimbingan, tuntunan, ilmu dan semangat dalam menyelesaikan tugas akhir ini dari awal hingga akhir. Terima kasih atas semua inspirasi untuk menyelesaikan penelitian Tugas Akhir ini, yang semula hanya berupa sebuah ide hingga mampu menjadi sebuah proposal. Hingga menjadi suatu karya Tugas Akhir yang utuh dan dapat diselesaikan.
2. Dosen penguji, Bapak Sholiq S.,T. dan Bapak Bekti Cahyo Hidayanto, S.Si., M.Kom, yang telah memberikan bantuan dalam memberikan saran dan masukan untuk menjadi perbaikan dan pelajaran dalam menyusun Tugas Akhir ini menjadi lebih baik

3. Bu Dr. Maria Anityasari, sebagai sosok Ibu pembimbing yang mengajarkan bahwa hidup ini jangan setengah-setengah untuk melakukan sesuatu tetapi berusahalah dengan semaksimal mungkin, "*Full Tilt*". Terima kasih atas dedikasi, waktu, dan pelajaran yang Ibu Maria berikan.
4. Bapak Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom selaku ketua jurusan Sistem Informasi ITS dan seluruh dosen serta karyawan di jurusan Sistem Informasi ITS.
5. Bapak Radityo Prasetianto Wibowo, S. Kom, M. Kom. selaku dosen wali yang telah memberikan bimbingan setiap melakukan perwalian untuk menentukan langkah yang perlu dipersiapkan untuk mengawali setiap semester awal dan dalam melakukan pengambilan Tugas Akhir pada semester tujuh ini.
6. Bapak Bimo Gumelar, selaku dosen proyek yang memberikan pelajaran baru untuk belajar dan mengasah kemampuan dalam menyelesaikan suatu permasalahan baru, serta memberikan inspirasi baru yang tanpa disadari sangat membantu dalam mengerjakan penelitian Tugas Akhir ini.
7. Sahabat terbaik, seperjuangan dan sepenanggungan yang tiada hentinya memberikan semangat dan dukungan agar bisa terselesaikannya pengerjaan Tugas Akhir ini, disaat sudah ada perasaan untuk menyerah dalam mengerjakan dan untuk tetap percaya dan bersemangat bahwa Tugas Akhir pasti akan selesai. Terima kasih Giovanny Praisukma Pertiwi, sahabat terbaik.
8. Sahabat yang memberikan warna untuk memaknai indahnya hidup menjadi seorang mahasiswa, merasakan bagaimana perjuangan seorang mahasiswa untuk menuntut ilmu untuk meraih secercah harapan baru. Terima kasih untuk Lukman Hendarwin atas warna baru untuk memulai pengerjaan Tugas Akhir ini.

9. Keluarga besar ITS International Office yang menjadi curahan untuk membangkitkan semangat baru untuk tetap bersemangat menjalani aktivitas sehari-hari menjadi lebih baik dan lebih baik lagi setiap harinya.
10. Medfo (Media dan Informasi) IO Team, yang selalu memberikan semangat dengan memberikan setiap pertanyaan mengenai kabar Tugas Akhir ini hingga dapat diselesaikan. Terima kasih Lucky Caesar, Fadhil Syah Putra, Mikhael Vidi, Putri Melati, Nayyiroh, Reinaldy Leopard.
11. Teman seperjuangan yang turut merasakan bagaimana menjadi seorang mahasiswa tingkat akhir yang sedang berusaha untuk meraih dan mewujudkan setiap mimpi-mimpinya. Terima kasih untuk Henny Kusumaningrum, Wike Eriyandari, Ivana Irene, Firza Amelia, Chafid, Bahalwan Apriansyah, Firman Faqih Nosa, Firdatun Nisa, Denisa.
12. Para senior yang memberikan inspirasi untuk kelak dapat mengikuti jejak mereka, Mbak Zatalini Marshall dan Mbak Adinda Moizara.
13. Seluruh teman seperjuangan di PPSI yang sama-sama merasakan bagaimana perjuangan dalam membuat Tugas Akhir yang telah memberikan dukungan dan bantuan yang tidak dapat disebutkan satu per satu. Serta Bapak Hermono yang telah banyak membantu dalam setiap proses persiapan melakukan sidang proposal hingga sidang akhir.
14. Mbak Az Zahra FS dan Mas Ikhsan Putra yang memberikan inspirasi dan begitu banyak masukan untuk menjadi semangat dalam melanjutkan studi.
15. BASILISK, angkatan 2011 Jurusan Sistem Informasi, ITS yang memberikan begitu banyak warna cerita selama menjalani masa kuliah untuk meraih gelar sarjana.
16. Kepada seluruh pihak yang tidak dapat disebutkan satu per satu yang telah memberikan banyak bantuan bagi penulis dalam menyelesaikan pengerjaan Tugas Akhir ini.

Tugas Akhir ini jauh dari kesempurnaan, sehingga masih banyak kekurangan yang menjadi pelajaran untuk dapat diperbaiki menjadi lebih baik. Oleh karena itu, mohon maaf atas segala kekurangan dan kekeliruan. Semoga tugas akhir ini dapat bermanfaat bagi seluruh pihak dan kritik dan saran yang membangun dapat menjadikan motivasi baru dalam melakukan penelitian selanjutnya.

Surabaya, 14 Januari 2015

Brigitta Devianti Cahyabuana

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

Bab ini menjelaskan tentang pendahuluan pengerjaan tugas akhir ini, yang meliputi latar belakang, rumusan permasalahan, batasan masalah, tujuan penelitian hingga manfaat yang diperoleh dari penelitian ini.

1.1. Latar Belakang

Jaringan bisnis semakin berkembang luas, teknologi informasi semakin berkembang pesat. Perusahaan pelaku bisnis memerlukan suatu media yang mampu memberikan kemudahan dalam menjalankan proses bisnis untuk mencapai keuntungan maksimal. Oleh karena itu di era globalisasi, penerapan teknologi informasi semakin menjadi tren dikalangan pelaku bisnis. Salah satunya penerapan teknologi informasi sebagai otomatisasi proses pengelolaan informasi.

Dunia perbankan mengalami peningkatan dalam melakukan inovasi penggunaan teknologi tiap tahunnya untuk memenuhi keinginan nasabah dan berlomba-lomba untuk menjadi yang pertama dalam inovasi penggunaan TI demi memenangkan persaingan pasar. Laporan *International Data Corporation* (IDC) memberikan daftar tahunan pada bank-bank di kawasan Asia/Pasifik mengenai penerapan insiatif untuk menerapakan strategi penggunaan teknologi informasi untuk dapat mengintegrasikan secara efektif. Penerapan teknologi informasi ini dibutuhkan managemen risiko yang memiliki persyaratan kepatuhan. Li-Mei Chew, *Associate Director* untuk IDC *Financial Insights* Asia/Pacifik memberikan komentar, “Terbukti risiko masih menjadi pertimbangan sangat penting pada tahun 2013, para eksekutif TI dipaksa untuk melakukan penilaian risiko baru yang ditimbulkan dari implementasi

dan penerapan teknologi informasi yaitu mengenai *social business, cloud, big data and mobile*".

Penggunaan teknologi informasi dalam mendukung proses bisnis perusahaan, harus diimbangi dengan manajemen risiko pada teknologi informasi yang digunakan. Dengan tujuan untuk meminimalisir kegagalan atau kerusakaan pada sistem. Sehingga dengan melakukan analisis risiko pada teknologi informasi yang digunakan dapat menghasilkan daftar risiko sebagai tindak pencegahan dari ancaman yang mungkin terjadi.

Manejemen Risiko adalah proses untuk mengidentifikasi, menganalisis, mengevaluasi, mengendalikan, mengawasi, dan mengkomunikasikan risiko secara logis dan sistematis yang bertujuan untuk meminimalisir kerugian dan memaksimumkan kesempatan (NewZealandStandards, 1999). Manejemen risiko perlu dilakukan oleh perusahaan karena telah banya ahli dan profesional memberikan pernyataan bahwa kegagalan bisa disebabkan oleh kekacauan dalam informasi risiko karena melakukan penilaian risiko dari perspektif yang berbeda (McCuaig, 2008).

Dalam melakukan analisis manajemen risiko diharapkan dapat menjawab lima pertanyaan (McCuaig, 2008):

1. Apa yang salah?
2. Bagaimana bisa salah?
3. Apa yang menyebabkan ancaman?
4. Apa yang bisa dilakukan dengan itu?
5. Bagaiamana cara penanganannya jika kejadian itu terulang kembali?

IDC Financial Insights Pivot Tabel menyediakan perkiraan mengenai *Worldwide Risk Information Technologies and Services* (RITS), terhadap risiko penerapan teknologi informasi dan layananan. Pasar RITS memperhitungkan penggunaan teknologi informasi

sebanyak $71.200.000.000 pada tahun 2014 dan akan bertambah hingga $87.400.000.000 pada tahun 2017. Persentase risiko dari belanja TI mencapai 16,5% dari total pengeluaran pada tahun 2014 dan akan bertambah hingga 18% pada tahun 2017 (Michael Versace, 2013).

Manajemen risiko dapat dilakukan dengan menggunakan beberapa metode, salah satu metode yang dapat digunakan ialah *Failure Mode and Effect Analysis* (FMEA). Metode FMEA membantu dalam melakukan analisis risiko hingga memberikan penilaian untuk pemrioritasan risiko. Namun, penerapan metode FMEA memiliki kelemahan jika diterapkan secara langsung dengan kondisi lingkungan perusahaan yang sebenarnya (Yeh & Hsieh, 2007).

Beberapa kelamahan penerapan metode FMEA :

1. Penggunaan kategori pada FMEA berdasarkan kategori "*high*", "*medium"*, dan "*low"* sulit dilakukan evaluasi secara tepat untuk mendefinisikan risiko dari segi reliabilitas dan keamanan sistem.
2. Penilian tiga parameter pada FMEA yaitu, "*severity"* (S), "*occurance"* (O), dan "*detection"* (D) diasumsikan memiliki tingkat kepentingan yang sama. Pada kondisi nyata, tingkat kepentingan dari tiga parameter ini tidak sama.
3. Prioritasasi risiko menggunakan *Risk Priority Number* (RPN) akan memberikan kemungkinan hasil yang berbeda untuk melakukan tindakan perbaikan dan melakukan pencegahan.
4. Pengerjaan analisis risiko menggunakan FMEA harus mempertimbangkan keragaman dan kemampuan setiap anggota tim FMEA.

Oleh karena itu, pentingnya analisis konsistensi hasil penilaian risiko menggunakan metode FMEA, agar dapat diterapkan sesuai dengan kebutuhan dan kondisi perusahaan. Penelitian mengenai penerapan konsistensi penggunaan metode FMEA menghasilkan beberapa modifikasi terhadap penggunaan analisis risiko metode FMEA. Agung Sutrisno dan Tzong-Ru (Jiun-Shen) Lee telah melakukan penelitian mengenai modifikasi FMEA untuk meningkatkan hasil *Risk Priority Number* (RPN) hingga melakukan prioritasi ulang (Sutrisno & Lee, 2011). Beberapa modifikasi FMEA yang dilkukan antara lain:

- Mark A. Moris melakukan penelitian terhadap menggunaan metode FMEA 4th edititon dengan menggunakan referensi tambahan dari AIAG (*Automotive Industry Action Group*), DFMEA (*Design FMEA*) dan PFMEA (*Process FMEA*) untuk menghasilkan penggunaan FMEA pada ASQ Automotive Division Webinar. Tujuan dari penelitian ini untuk menjelaskan tujuan, keuntungan, dan sasaran FMEA; memilih tim yang berkompeten untuk melakukan analisis risiko menggunakan FMEA, mengembangkan dan memenuhi FMEA, melakukan tinjauan, kritik, dan perbaruan dari FMEA yang telah ada, mengatur kegiatan tindak lanjut dan verifikasi dari penggunaan FMEA, mengembangkan FMEA yang sesuai dengan referensi AIAG FMEA (Morris, 2011).
- Pemahaman dan penerapan fundamental FMEA yang dilakukan oleh Carl S. Carlson dari ReliaSoft Corporation dengan tujuan untuk memberikan penjelasan mengenai konsep dan prosedur

penggunaan FMEA secara efektif dengan enam sukses faktor pada penggunaan FMEA (Carlson, 2014).

- Penggunaan FMEA dimulai pada tahun 1940an di Amerika Serikat pada bidang manufaktur. Kini, penggunaan FMEA juga digunakan pada industri perbankan. Bank membutuhkan pengembangan produk yang cepat dengan kualitas terbaik yang dapat meningkatkan kualitas dari loyalitas pelanggan. Kunci untuk meningkatkan pengembangan kualitas pada komponen produk dan kebutuhan bisnis yang membutuhkan pengujian prioritas tertinggi melalui penggunaan metode FMEA (Gundry, 2014).

Berdasarkan penelitian terdahalu terhadap modifikasi FMEA, penelitian ini bertujuan untuk melakukan analisis konsistensi penilaian risiko menggunakan metode FMEA dengan cara melakukan analisis kesenjangan pada hasil penilaian risiko. Hasil akhir dari tugas akhir ini adalah membuat rekomendasi perbaikan metode FMEA yang cocok dengan kondisi perusahaan XYZ. Kondisi perusahaan XYZ menginginkan suatu analisis risiko yang didasarkan pada pentingnya memperhatikan faktor tingkah laku untuk meminimalisir risko penggunaan teknologi informasi yang ada. Sehingga faktor tingkah laku menjadi rekomendasi perhitungan risiko dalam melakukan risiko yang sesuai dengan kondisi perusahaan XYZ.

1.2. Rumusan Permasalahan

Berdasarkan latar belakang, maka dirumuskan beberapa permasalahan yaitu :

1. Apa hasil identifikasi dan penilaian risiko teknologi informasi pada perusahaan XYZ menggunakan metode FMEA?
2. Apakah penilaian peringkat risiko dengan menggunakan metode FMEA memberikan hasil yang konsisten?
3. Bagaimana hasil kerangka FMEA yang disesuaikan yang cocok dengan kondisi dan kebutuhan perusahaan XYZ?

1.3. Batasan Masalah

Batasan masalah yang digunakan pada penyusunan laporan ini meliput :

1. Hasil identifikasi dan penilaian risiko teknologi informasi pada perusahaan XYZ dengan menggunakan metode FMEA.
2. Membuktikan konsistensi penilaian risiko teknologi informasi pada perusahaan XYZ dengan menggunakan perbandingan hasil penilaian risiko dari penilaian dua tim berbeda menggunakan metode FMEA.
3. Membuat rekomendasi kerangka FMEA yang disesuaikan dengan kondisi perusahaan XYZ untuk melakukan penilaian risiko teknologi informasi.
4. Penelitian hanya menganalisis konsistensi hasil penggunaan metode FMEA dalam melakukan manajemen risiko TI pada perusahaan XYZ.

1.4. Tujuan Penelitian

Tujuan penyusunan laporan ini :

1. Menghasilkan identifikasi risiko teknologi informasi pada perusahaan XYZ.
2. Menghasilkan hasil dari konsistensi penerapan metode FMEA dalam melakukan penilaian risiko.
3. Menghasilkan kerangka FMEA yang disesuaikan dengan kebutuhan perusahaan XYZ.

1.5. Manfaat Penelitian

Manfaat yang didapat dari penelitian ini adalah:

1. Perusahaan mendapatkan informasi mengenai risiko teknologi informasi yang ada pada perusaahaan XYZ.
2. Memberikan hasil konsistensi dari penerapan metode FMEA dalam melakukan penilaian risiko.
3. Menghasilkan penyebab konsistensi perbedaan hasil pada penilaian peringkat risiko metode FMEA.
4. Menghasilkan kerangka risiko teknologi informasi baru yang sesuai dengan kondisi dan kebutuhan perusahaan XYZ.

1.6. Sistematika Penulisan

Sistematika penulisan dari penelitian ini adalah sebagai berikut :

BAB I. PENDAHULUAN

Pendahuluan berisikan mengenai bahasan latar belakang penelitian, rumusan permasalahan, batasan masalah, tujuan dan manfaat penelitian

serta sistematika penulisan dalam buku penelitian.

BAB II. TINJAUAN PUSTAKA

Tinjauan Pustaka berisikan mengenai bahasan tinjauan pustaka atau literatur yang digunakan dalam penelitian ini. Literatur yang digunakan adalah risiko, manajemen risiko, metode FMEA, konsistensi penilaian risiko menggunakan metode FMEA.

BAB III. METODOLOGI PENELITIAN

Metodologi Penelitian membahas mengenai metode penelitian atau langkah-langkah yang dilakukan dalam penelitian untuk mencapai tujuan penelitian yang telah ditetapkan.

BAB IV. KONSISTENSI PENILAIAN RISIKO MENGGUNAKAN METODE FMEA

Konsistensi Penilaian Risiko Menggunakan Metode FMEA, membahas mengenai analisis risiko pada penggunaan teknologi informasi pada teller Bank XYZ, penilaian risiko menggunakan metode FMEA, hingga pemrioritasan risiko untuk menghasilkan prioritasisasi risiko yang memiliki tingkat risiko paling tinggi. Dari hasil prioritisasi risiko kemudian dilakukan analisis konsistensi penilaian risiko yang telah dilakukan oleh dua tim berbeda pada studi kasus yang sama untuk menjawab apakah sudah konsisten atau belum kah penggunaan metode FMEA.

BAB V. PEMBAHASAN KERANGKA FMEA YANG DISESUAIKAN

Pembahasan Kerangka FMEA yang Disesuaikan menjelaskan mengenai setiap fase dari kerangka FMEA yang disesuaikan dengan kebutuhan dan kondisi perusahaan dalam melakukan analisis risiko untuk memberikan prioritisasi risiko.

BAB VI. PENUTUP

Penutup, menjelaskan mengenai kesimpulan dari penelitian, serta memberikan saran perbaikan untuk penelitian selanjutnya, agar kualitas dari penelitian dapat terus meningkat dan dapat dikembangkan.

BAB II
TINJAUAN PUSTAKA

Tinjauan pustaka menjelaskan mengenai studi literatur yang digunakan untuk melakukan penelitian "Konsistensi Penggunaan Metode FMEA terhadap Penilaian Risiko Teknologi Informasi".

2.1. Risiko

Risiko adalah hal yang dapat dihindari pada suatu kegiatan atau aktivitas yang dapat dilakukan manusia dan terdapat ketidakpastian serta *probability* yang memiliki dampak. Menurut para ahli risiko adalah sebagai berikut :

- Risiko adalah variansi dari hasil yang terjadi selama periode tertentu dan pada kondisi tertentu (William dan Heins, 1985).
- Risiko adalah sebuah potensi suatu variasi yang memiliki sebuah hasil (William, Smith, Young, 1995).

2.2. Risiko pada Teknologi Informasi

Risiko pada penggunaan teknologi informasi akan menjadi semakin besar jika dibandingkan dengan suatu proses bisnis yang dilakukan secara manual tanpa menggunakan penerapan teknologi informasi. Pernyataan ini didukung oleh pernyataan yang dikemukakan oleh Warran McFarlan mengenai tingkat risiko dalam melaksanakan proyek sistem informasi. Ancaman pada penggunaan teknologi informasi, yaitu kegagalan pada hardware dan software seperti kehilangan data, malware, virus, *spam, phishing,* hingga *human error*. Ancaman kriminal pada penggunaan teknologi informasi seperti adanya peretas, penipuan, pencurian password, penolakan

layanan, pelanggaran keamanan, karyawan yang tidak jujur (Goverment, 2014).

2.3. Manajemen Risiko

Suatu cara untuk memberikan dalam mengidentifikasi, mengolah risiko hingga memberikan penilaian risiko secara efektif untuk mengantisipasi ancaman pada perusahaan disebut dengan kegiatan manajemen risiko. Sistem pada manajemen risiko adalah untuk melakukan Manajemen Risiko adalah suatu cara untuk mengkordinir dan mengawasi jalannya proses bisnis perusahaan melalui pendekatan risiko (ISO 31000:2009). Proses manajemen risiko dilakukan dengan cara mengidentifikasi, menilai, dan menentukan risiko, serta bagaiaman rindakan yang perlu dilakukan dalam melakukan antisipasi dan melakukan pemantauan terhadap risiko yang mungkin terjadi, hal ini disampaikan oleh H.M. Treasury.

2.4. Manajemen Risiko Teknologi Informasi

Manajemen risiko teknologi informasi dilakukan dengan tujuan untuk mengelola penggunaan teknologi informasi untuk mengidentifikasi risiko terkait dengan penerapan teknologi informasi. Manajemen risiko teknologi informasi dilakukan dengan upaya untuk meminimalisir risiko dan mengelola investasi teknologi informasi yang telah dilakukan. Berbagai para ahli dan profesional yang telah menerapkan manajemen risiko memberikan kesimpulan bahwa kegagalan yang terjadi disebabkan oleh kekacauan informasi risiko karena penilaian risiko yang dilakukan dari perspektif yang berbeda (Mccuaig, 2008).

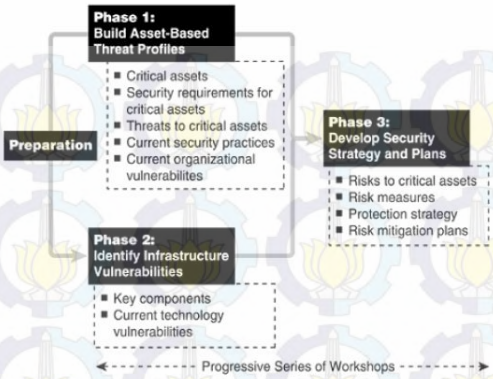
2.5. OCTAVE

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) merupakan salah satu kerangka untuk melakukan pendekatan standarisasi untuk pengendalian risiko terkait dengan keamanan informasil. Sehingga metode ini digunakan untuk mengidentifikasi aset informasi yang penting pada perusahaan (Christopher J. Alberts, 1999).
Metode yang digunakan OCTAVE dengan beberapa kunci karakteristik yaitu :

- Terdiri dari tim kecil yang bekerja bersama untuk mengamankan aset perusahaan dari ancaman.
- Dirancang dengan fleksibel bisa digunakan untuk penanganan risiko lingkungan pada perusahaan, kebutuhan keamanan, dan level dari kemampuan.
- Bertujuan untuk operasional risiko yang didasarkan pada pandangan keamanan dan pemakaian teknologi pada konteks bisnis.

OCTAVE memerlukan katalog informasi untuk membuat pengukuran kinerja perusahaan, menganalisa ancaman, dan membangun stretegi proteksi. Katalog ini dijadikan sumber referensi, yaitu meliputi :

- *Catalog of Practice* : Katalog mengenai strategi dan praktek keamanan informasi.
- *Catalog Threat Profile* : Katalog mengenai sumber ancaman secara umum pada perusahaan.
- *Catalog of Vulnerabilites* : Katalog mengenai masalah-masalah yang menjadi kelemahan pada keamaan informasi pada perusahaan.



Gambar 2.5.1. Tahapan pada OCTAVE

Tahapan pada OCTAVE :

1. *Preparation*

   Tahapan persiapan untuk melakukan metode OCTAVE dengan cara menyusun jadwal, membentuk tim analisis, serta meminta dukungan dan menyiapkan keperluan dalam melakukan analisis.
2. Fase 1 : *Build Asset-Based Thread Profile*

   Pada fase ini tim akan melakukan identifikasi pada kriteria dampak evaluasi untuk mengevaluasi risiko, mengidentifikasi aset perusahaan, dan mengevaluasi keamanan yang ada pada perusahaan. Harapannya mampu mengidentifikasi keamanan dan ancaman pada aset perusahaan.
3. Fase 2 : *Identify Infrastucture Vulnerabilities*

   Pada fase 2 ini akan dilakukan analisa untuk menentukan *high level review* dengan berfokus pada keamanan infrastruktur sehingga menghasilkan kompenen dalam mengatur dan memelihara infrastruktur.
4. Fase 3 : *Develop Security and Plans*

   Pada fase 3, tim akan mengidentifikasi risiko ke aset kritis perusahaan untuk segera membuat keputusan

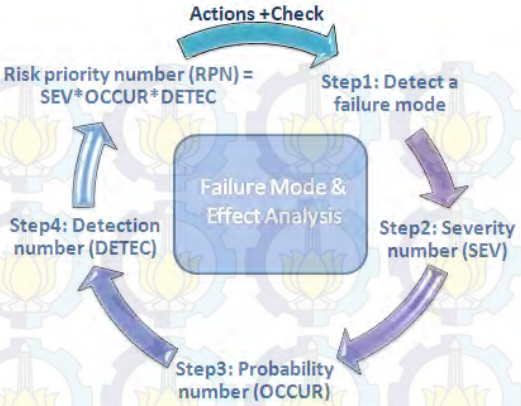
dengan tujuan terhadap perlindungan perusahaan dalam mengurangi dan mengatasi risiko.

Hasil dari penggunaan OCTAVE :

1. Strategi perlindungan organisasi yang luas:
   Strategi perlindungan menguraikan secara singkat arah organisasi dengan mematuhi praktik keamanan informasi.
2. Rencana mitigasi risiko: Rencana ini dimaksudkan untuk mengurangi risiko aset kritis untuk meningkatkan praktik keamanan yang di pilih.
3. Daftar tindakan: termasuk tindakan jangka pendek yang dibutuhkan untuk menunjukkan kelemahan yang spesifik.
4. Daftar informasi penting terkait dengan aset yang mendukung tujuan bisnis dan sasaran organisasi.
5. Hasil survei menunjukkan sejauh mana organisasi mengikuti praktik keamanan yang baik.
6. Profil risiko untuk setiap aset kritis menggambarkan jarak antara risiko terhadap aset.

2.6. Metode FMEA (Failure Mode and Effect Analysis)

FMEA adalah suatu alat yang secara sistematis mengidentifikasi akibat atau konsekuensi dari kegagalan sistem atau proses, serta mengurangi atau mengeliminasi peluang terjadinya kegagalan. Analisis pengaruh dan mode kegagalan risiko (*risk FMEA*) adalah cara utama untuk melakukan penghitungan pada manajemen risiko (Gaspersz). FMEA adalah teknik analisis untuk mengidentifikasi dan mengeliminasi potensi dari kegagalan, permasalahan, kerusakan pada sistem, desain, proses, atau layanan (Stamatis, 1995).



Gambar 2.6.1. Metode FMEA (Failure Mode and Effect Analysis) (Sumber: FMEA, 2014)

Tahapan dari penilaian menggunakan FMEA adalah sebagai berikut:

1. Identifikasi sistem dan elemen sistem dan kegagalan dari efek yang ditimbulkan.
2. Menentukan tingkat keparahan efek dari suatu kegagalan (*severity*).
3. Menentukan frekuensi kemungkinan risiko terjadi (*occurence*).
4. Menentukan tingkat Deteksi yang telah dilakukan dalam mencegah risiko (*Detection*).
5. Menghitung *Risk Priority Number* (RPN) yang menyatakan tingkat risiko dari suatu kegagalan. Angka RPN berkisar antara 1 – 1000, semakin tinggi angka RPN maka semakin tinggi risiko suatu potensi kegagalan terhadap sistem, desain, proses maupun pelayanan. RPN = *Severity* x *Occurrence* x *Detection*.

6. Memberikan rekomendasi tindakan yang dapat diterapkan untuk mengurangi tingkat risiko kegagalan..

2.6.1. Petunjuk Pemberian Skor Dampak (*Severity* = S)

Petunjuk pemberian skor pada kategori *Severity (Impact)* bertujuan untuk melihat dampak atau pengaruh besar risiko terhadap aspek-aspek tujuan proyek, meliputi jadwal *(timeline),* biaya (*cost*) dan teknikal (*technical / operational*).

Tabel 2.1.1. Skor Dampak (Sumber: FMEA)

Effect	*Severity of Effect*	*Ranking*
Hazardous: without warning	Potensial kegagalan atau risiko mempengaruhi keamanan sistem tanpa peringatan	10
Hazardous: with warning	Potensial kegagalan atau risiko mempengaruhi keamanan sistem dengan peringatan	9
Very high	Tidak dapat dioperasikan dengan kegagalan yang merusak tanpa mengorbankan keamanan	8
High	Tidak dapat dioperasikan dengan kerugian atau kerusakan peralatan	7
Moderate	Tidak dapat dioperasikan dengan kerugian kecil (Proses)	6
Low	Tidak dapat dioperasikan tanpa kerugian (Prosedur)	5

Effect	*Severity of Effect*	*Ranking*
Very Low	Penurunan Kinerja secara signifikan (*Policy*)	4
Minor	Penurunan Kinerja	3
Very Minor	Efeknya kecil	2
None	Tidak ada memiliki efek	1

2.6.2. Petunjuk Pemberian Skor Kemungkinan (*Occurence* = O)

Petunjuk pemberian skor pada kategori *Occurance (Likelihood)* bertujuan untuk mengidentifikasi kemungkinan terjadinya sebuah risiko.

Tabel 2.2.1. Skor Likelihood (Sumber: FMEA)

Probability of Failure	*Possible Failure Rate*	*Ranking*
Very High: Failure is almost ineviTabel	Lebih dari 1 kali terjadi setiap harinya	10
High: Failures occur almost as often as not	1 kali terjadi setiap tiga hingga empat hari	9
High: Repeated Failures	1 kali terjadi setiap minggu	8
High: Failures occur often	1 kali terjadi setiap bulan	7
Moderately High:	1 kali terjadi setiap tiga bulan	6

Probability of Failure	*Possible Failure Rate*	*Ranking*
Frequent Failure		
Moderately: Kadang-kadang kegagalan	1 kali terjadi setiap enam bulan	5
Moderately Low: Infrequent Failure	1 kali terjadi setiap tahun	4
Low: Relatively few failures	1 kali terjadi setiap satu hingga tiga tahun	3
Low: Relatively few failures and far between	1 kali terjadi setiap tiga tahun hingga lima tahun	2
Remote: failure is unlikely	1 kali terjadi lebih dari lima tahun	1

2.6.3. Petunjuk Pemberian Skor Deteksi (*Detection* = D)

Petunjuk pemberian skor pada kategori *Detection* bertujuan untuk mengukur tingkat efektivitas metode atau kemampuan untuk mendeteksi terjadinya suatu risiko. Deteksi dilakukan untuk melihat bagaiamana cara mendeteksi peristiwa yang memiliki risiko secara tepat, agar perusahaan mampu membuat tindakan terhadap risiko yang terdeteksi secara cepat.

Tabel 2.3.1. Skor Deteksi (Sumber: FMEA)

Detection	*Criteria: Likelihood of Detection*	*Ranking*
Absolutely Uncertainty	Kekurangan tidak dapat di deteksi penyebabnya	10
Very Remote	Melakukan sample atau pemeriksaan untuk mencek cacat atau kekurangan	9

Detection	*Criteria: Likelihood of Detection*	*Ranking*
Remote	Produk diterima berdasarkan ketidakcacatan dalam sample	8
Very Low	Semua produk diperiksa secara manual dalam proses	7
Low	Produk diinspeksi manual menggunakan mistake-proofing modification	6
Moderate	SPC (Statistical Process Control) digunakan dalam proses dan produk adalah final inspeksi	5
Moderately High	Kemampuan alat kontrol untuk mendeteksi bentuk dan penyebab kegagalan sedang sampai tinggi	4
High	Kemampuan alat kontrol untuk mendeteksi bentuk dan penyebab kegagalan tinggi	3
Very High	Semua produk secara otomatis diperiksa	2
Almost Certain	Kekurangan atau kecacatan sudah jelas dan dapat dicegah dari customer	1

2.6.4. Penentuan Level Risiko

Metode FMEA memberikan metode perhitungan risiko dengan cara membuat nilai prioritasi risiko, *Risk Priority Number* (RPN). Tahapan ini setelah menentukan nilai *severity*, *occurrence* dan *detection* maka didapatkan nilai RPN untuk masing-masing risiko yang ada. Berikut ini merupakan penentuan level risiko berdasarkan nilai RPN :

Tabel 2.4.1. Penentuan Level Risiko (Sumber: FMEA)

Level Risiko	Skala Nilai RPN
Very low	x < 20
Low	20≤ x <80
Medium	80≤ x <120
High	120≤ x <200
Very high	x>200

Dengan adanya pengkategorian RPN, maka dapat diketahui risiko yang memiliki nilai RPN tinggi masuk pada kategori *very high* sehingga dapat dijadikan prioritas dalam menentukan tindakan antisipasi, mitigasi dan strategi terhadap risiko yang memiliki tingkatan paling tinggi, sehingga operasional bisnis perusahaan dapat tetap berjalan dengan optimal meskipun terjadi gangguan atau bencana.

2.7. Konsistensi Penggunaan FMEA

Konsistensi penggunaan FMEA mengakibatkan beberapa versi yang dilakukan modifikasi terhadap model FMEA yang sudah pernah dilakukan oleh berbagai peneliti. Beberapa penelitian yang telah berupaya mengembangkan modifikasi FMEA ini, anatara lain (Narayanagounder & Gurusami, 2009) :

- Rhee dan Ishii (2003) mempresentasikan biaya hidup berdasarkan FMEA untuk melakukan pengukuran risiko pada biaya selama masa hidup. Biaya hidup berdasarkan FMEA digunakan untuk membandingkan dan memilih alternatif desain yang dapat mengurangi biaya siklus hidup keseluruhan pada suatu keadaan tertentu. Simulasi Monte Carlo digunakan untuk melakukan analisis sensitivitas pada variabel yang mempengaruhi biaya siklus

hidup. Sebuah studi kasus dilakukan pada skala akselerator partikel besar untuk meramalkan kegagalan biaya siklus hidup, untuk mengukur risiko, untuk merencanakan pencegahan dan melakukan pemeliharaan terjadwal dan pada akhirnya untuk meningkatkan *uptime* (Rhee & Ishii, 2003).

- John B. Bowles dan C Enrique Pelaez (1995) membuat usulan baru bagaimana cara melakukan *Failures Mode Effects and Critically Analysis* (FMECA) menggunakan teknik baru berdasarkan logika *fuzzy*. Anggota *fuzzy set* mewakili S, O, dan D untuk menilai kegagalan dalam FMECA. Hubungan antara risiko dan S, O, D dijelaskan dengan cara *if-then rules* pada fuzzy kemudian peraturan diekstrasi dari pengetahuan opara ahli dan perarturan dasar para ahli. Peringkat untuk S, O dan D kemudian dikombinasikan untuk mencocokkan premis setiap kemungkinan pada aturan *if-then* dan kemudian dievaluasi dengan inferensi minimum-maksimum. Kesimpulan Fuzzy adalah *finally defuzzified* oleh rata-rata tertimbang dari metode maksimum untuk menilai tingkat risiko kegagalan (Bowles & Pelaez, 1995).
- Teng, SH dkk (1996) membuat usulan mengenai isu-isu keandalan produk harus disertakan sebelum selesainya tahap desain dan harus mengkonfirmasi desain yang memiliki persyaratan terpenuhi. Cara untuk menerapkan FMEA ialah dengan membuat laporan FMEA untuk kualitas sistem secara keseluruhan. Akan tetapi, cara ini tidak hanya sulit

untuk membuat laporan FMEA, tetapi juga penggunaan informasi kualitas sistem secara keseluruhan untuk memperbaiki produk dan rancangan desain (Teng & Ho, 1996).

- Arunachalam dan Jegadheesan (2006) mengusulkan FMEA dimodifikasi dengan keandalan dan pendekatan berbasis biaya untuk mengatasi kelemahan dari FMEA tradisional. Studi kasus dilakukan dengan keandalan dan pendekatan berbasis biaya untuk sistem pendingin kendaraan angkutan penumpang menggunakan data yang dikumpulkan dari negara depot perusahaan transportasi (Arunachalam & Jegadheesan, 2006).
- Franceschini dan Galetto (2001) mengembangkan metodologi unik untuk menentukan tingkat prioritas risiko untuk mode kegagalan di FMEA. FMEA yang telah dikembangkan ini mampu menghadapi situasi yang memiliki tingkat kepentingan yang berbeda untuk tiga komponen indeks mode kegagalan, yaitu keparahan, kejadian, dan deteksi (Franceschini & Galetto, 2001).
- Devadasan et al., (2003) berpendapat bahwa integrasi FMEA belum memberikan dampak bagi perbaikan lingkungan tim yang ada. Oleh karena itu, organisasi-organisasi ini tidak mencapai kualitas yang maksimal dari penggunaan aplikasi FMEA. Prinsip FMEA yang efektif dan membantu untuk mencapai peningkatan mutu berkelanjutan, tetapi tidak praktis dalam mengimplementasikan pada lingkungan yang sebenernya. Devadasan et al. (2003)., mengusulkan versi modifikasi dari FMEA

dikenal sebagai *Total Failure Mode Effects Analysis* (TFMEA) untuk melaksanakan pencegahan kegagalan holistik untuk mencapai perbaikan kualitas yang berkesinambungan (Devadasan, Muthu, Samson, & R.A., 2003).

- Chen (2007) mengevaluasi struktur hirarki dan tingkat saling ketergantungan dari tindakan korektif dengan menggunakan *Interpretive Structural Model* (ISM). Kemudian, perhitungan dilakukan untuk menentukan *weight of corrective actions* melalui *Analytic Network Process* (ANP). ANP digabungkan dengan utilitas dari tindakan korektif untuk membuat keputusan tentang urutan prioritas peningkatan FMEA menggunakan *Utility Priority Number* (UPN) (Chen, 2007)

2.8. Analisis Konsistensi Metode FMEA

Analisis risiko menggunakan metode FMEA menghasilkan penilaian pada risiko yang terjadi dari segi *severity*, *occurency*, dan *detection* dari setiap risiko. Konsistensi dari pemberian nilai pada risiko menggunakan metode FMEA ini perlu dilakukan eksplorasi untuk menganalisis kemungkinan terjadi perbedaan pada penilaian tiap risiko yang sudah pernah dilakukan oleh M.T. Oldehofa. (M.T. Oldenhofa J. v.-R., 2011).

Metode yang dilakukan oleh M.T. Oldehofa dalam menganilisis konsistensi metode FMEA dengan cara :

Gambar 2.8.1. Analisis Konsistensi Metode FMEA (Sumber: M. T. Oldenhofa, 2011)

2.8.1. Analisis Risiko

Analisis risiko teknologi informasi yang digunakan dinilai dari dua sudut pandang yang berbeda dimana dilakukan oleh dua tim yang berbeda dalam melakukan penilaian risiko.

2.8.2. Pemberian Nilai Risiko (*Severity, Occurence,* dan *Detection*)

Pemberian nilai risiko berdasarkan parameter *severity, occurence,* dan *detection* dari tiap-tiap risiko.

2.8.3. Pemrioritasan Penilaian Risko yang Dilakukan oleh Dua Tim Berbeda

Risiko yang telah dinilai menggunakan parameter *severity*, *occurence*, dan *detection* akan dilakukan pemrioritasan risiko yang memiliki urgensi tertinggi.

Pemrioritasan penilaian risiko menggunakan RPN, sehingga didapatkan hasil risiko yang telah dikategorikan berdasarkan level risiko (*very high, high, medum, low,* dan *very low*).

Penelitian analisis konsistensi risiko dengan cara membuat dua tim yang berbeda untuk mengidentifikasi risiko yang sama pada satu perusahaan. Kemudian membandingkan hasil peniliaian yang didapatkan apakah sudah konsisten atau belum

2.8.4. Perbandingan Hasil Penilaian Risiko

Hasil penilaian risiko yang dilakukan dari dua sudut pandang yang berbeda pada studi kasus perusahaan yang sama. Penelitian dilakukan dengan cara membuat perbandingan dalam melakukan penilaian risiko pada satu perusahaan yang dilakukan oleh dua tim yang berbeda. Kemudian, hasil penilaian risiko dilakukan perbandingan. Sehingga mendapatkan kesimpulan konsistensi penilaian risiko menggunakan metode FMEA.

2.9. Analisis Kesenjangan

Analisis kesenjangan adala suatu cara untuk menentukan perbedaan antara pengetahuan saat ini atau praktek yang dilakukan. Analisis kesenjangan akan memberikan informasi kesenjangan yang ada pada pengetahuan, keterampilan, atau praktek secara langsung (Janneti, 2012). Analisis kesenjangan merupakan sebuah alat yang digunakan untuk mengevaluasi kinerja. Analisis kesenjangan sering digunakan di bidang manajemen dan menjadi salah satu alat yang digunakan untuk mengukur kualitas pelayanan (*quality of services*).

Gap analysis diartikan sebagai suatu metode pengukuran bisnis yang memudahkan perusahaan untuk membandingkan kinerja aktual dengan kinerja

potensialnya. Dengan kata lain, *gap analysis* merupakan suatu metode yang digunakan untuk mengetahui kinerja dari suatu sistem yang sedang berjalan dengan sistem standar. Dalam kondisi umum, kinerja suatu institusi dapat tercermin dalam sistem operational maupun strategi yang digunakan oleh institusi tersebut.

2.10. Pendekatan Kualitatif

Metode penelitian yang digunakan dalam penelitian konsistensi penggunaan FMEA ini, menggunakan metode kualitatf untuk menjelaskan dan memahami masalah-masalah yang menjadi fokus masalah pada penelitian ini. Menurut Bodgan dan Taylor yang dikutip oleh Lexi J. Moleong, pendekatan kualitatif adalah sebuah prosedur dasar penelitian untuk menghasilkan data deskriptif secara tertulis ataupun secara lisan dari hasil pengamatan (Moleong, 2007). Perbedaan penelitian kualitatif dengan penelitian kuantitatif adalah penelitian kualitatif untuk mencari bentuk dan isi dari tindakan atau perilaku manusia dan untuk menganalisis kualitas dari tindakan dan perilaku manusia (Lindlof, 2002). Penelitian kualitatif adalah cara melakukan penyelidikan dan pemahaman untuk menjelaskan pemasalahan sosial atau manusia dimana dapat dilakukan dengan cara menjelaskan sebuah keadaan, gambaran holigstik, analisis kata-kata, laporan secara detail dari sudut pandang informan dan mempelajari kondisi sekitar (Creswell, 1994). Perbedaan model penelitian kuantitatif dan kualitatif (Neuman, 1997) :

Tabel 2.4.1. Model Penelitian Kuantitatif dan Kualitatif (Sumber: Neuman, 1997)

Kuantitatif	Kualitatif
Mengukur fakta-fakta objektif	Mengkonstruksikan realitas dan makna kultural

Kuantitatif	Kualitatif
Fokus pada variabel-variabel	Fokus pada proses dan peristiwa secara interaktif
Reliabilitas adalah kunci	Otentitas adalah kunci
Bebas nilai	Hadirnya nilai secara eksplisit
Bebas dari konteks	Dibatasi situasi
Banyak kasus dan subjek	Sedikit kasus dan subjek
Analisis statistik	Analisis tematik
Peneliti terpisah	Peneliti terlibat

Penelitian kualitatif memiliki ciri-ciri khusus antara satu penelitian dengan penelitian kualitatif lainnya. Hal ini disampaikan oleh John W. Creswell (Creswell, 1994), yaitu:

1. Penelitian dilakukan dengan pengaturan alami (*field focused*) untuk menggali dan mendapatkan sumber data. Peneliti tidak melakukan intervesi terhadap sumber informasi, seperti mempengaruhi opini, memaksa sumber bertutur, atau tidak berusha melayani informan secara empatetis.
2. Peneliti merupakan sumber instrumen dalam melakukan pengumpulan data untuk membangun validitas data.
3. Kumpulan data diungkapkan menjadi rangkaian kata-kata atau gambar.
4. Hasil penelitian harus menjelaskan tentang proses dari pada produk.
5. Peneliti kualitatif lebih tertatik pada bagian-bagian yang bersifat mikro untuk melakukan analisis data secara induktif.
6. Pemilihan bahasa yang ekspresif yang digunakan dalam menyampaikan hasil pengumpulan data.

7. Kemampuan penyajian secara persuasif dengan menampilkan alasan-alasan atau argumen yang berguna.

Rancangan penelitian pendekatan kualitatif yang telah dilakukan oleh John W. Cresswell dalam bukunya *Research Design: Qualitative and Quantitative Approaches* (Creswell, 1994) memiliki alur analisis data sebagai berikut:

Gambar 2.10.1. Penelitian Pendekatan Kualitatif (Sumber: Creswell, 1994)

- **Pernyataan informan**, peneliti mengumpulkan sebanyak-banyaknya data dan informasi terkait pengalaman, pengetahuan, serta pendapat informan dengan kaitannya untuk mendapatkan informasi sebagai bahan dari penelitian yang dilakukan.
- **Data pernyataan memiliki makna**, peneliti melakukan pencarian data dari pernyataan bermakna yang didapatkan dari informasi yang disampaikan informan. Cara yang dilakukan dalam menganalisis data pernyataan bermakna dengan melakukan reduksi terhadap data dan informasi yang ada.

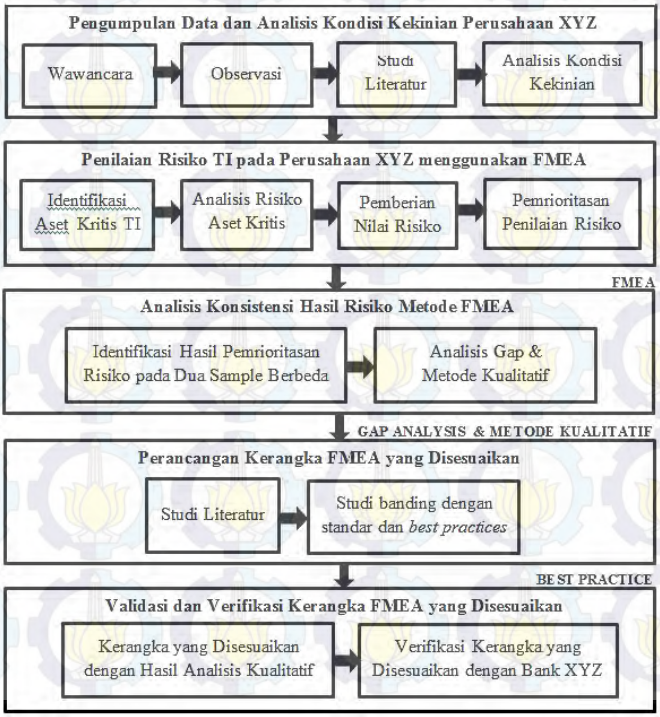
- **Identifikasi kategori yang muncul**, dilakukan identifikasi pada kategori-kategori yang mucul dari hasil pengumpulan data dan informasi dari informan untuk memudahkan dalam melakukan analisis.
- **Deskripsi kategori yang muncul**, penjelasan mengenai detail dari kategori-kategori yang muncul untuk memberikan informasi yang detail mengenai pengkategorian yang telah dilakukan pada setiap kategori yang ada.
- **Pengelompokan kategori utama**, pada tahap ini dilakukan pengelompokan kategori utama berdasarkan kategori yang telah ditentukan pada penelitian.
- **Proposisi minor**, pernyataan bermakna dari setiap kategori utama yang digunakan pada penelitian berdasarkan informasi yang ada. Pada tahap ini dibuat pernyataan kesimpulan pada setiap kategori berdasarkan informasi yang diperoleh pada penelitian.
- **Proposisi mayor**, pernyataan kesimpulan secara umum berdasarkan kesimpulan yang diperoleh pada proposisi minor. Pada tahap ini dibuat kesimpulan secara umum berdasarkan proposisi minor yang telah ditemukan pada penelitian.

BAB III
METODOLOGI PENELITIAN

Metodologi pengerjaan tugas akhir ini adalah untuk mengetahui hasil penilaian risiko menggunakan metode FMEA apakah memberikan hasil yang konsisten atau tidak. Dan kemudian dibuat Kerangka FMEA yang Disesuaikan yang bertujuan untuk menghasilkan penilaian risiko menggunakan metode FMEA yang konsisten. Tahapan untuk melakukan metodologi penelitian ini terbagi menjadi dua, yaitu Metode Konsep Pengerjaan dan Metode Pengerjaan.

3.1. Metode Konsep Pengerjaan

Metode konsep pengejaan tugas akhir :

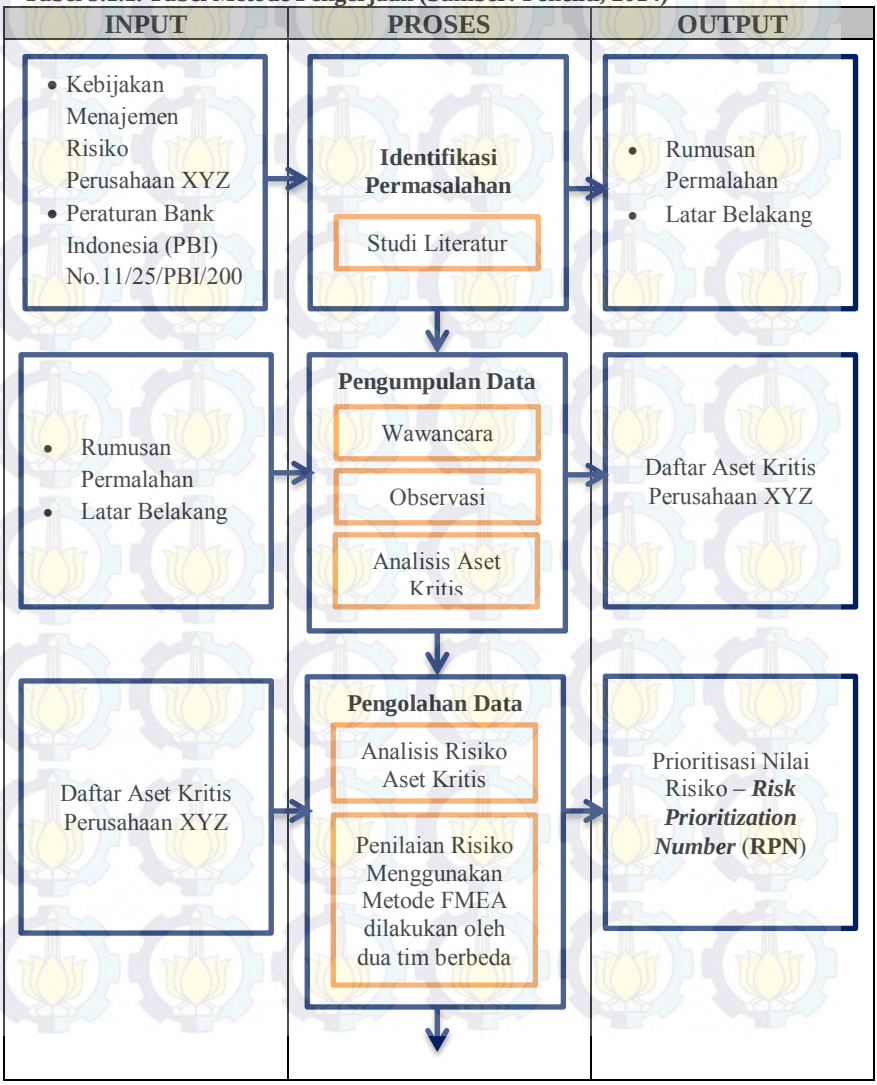


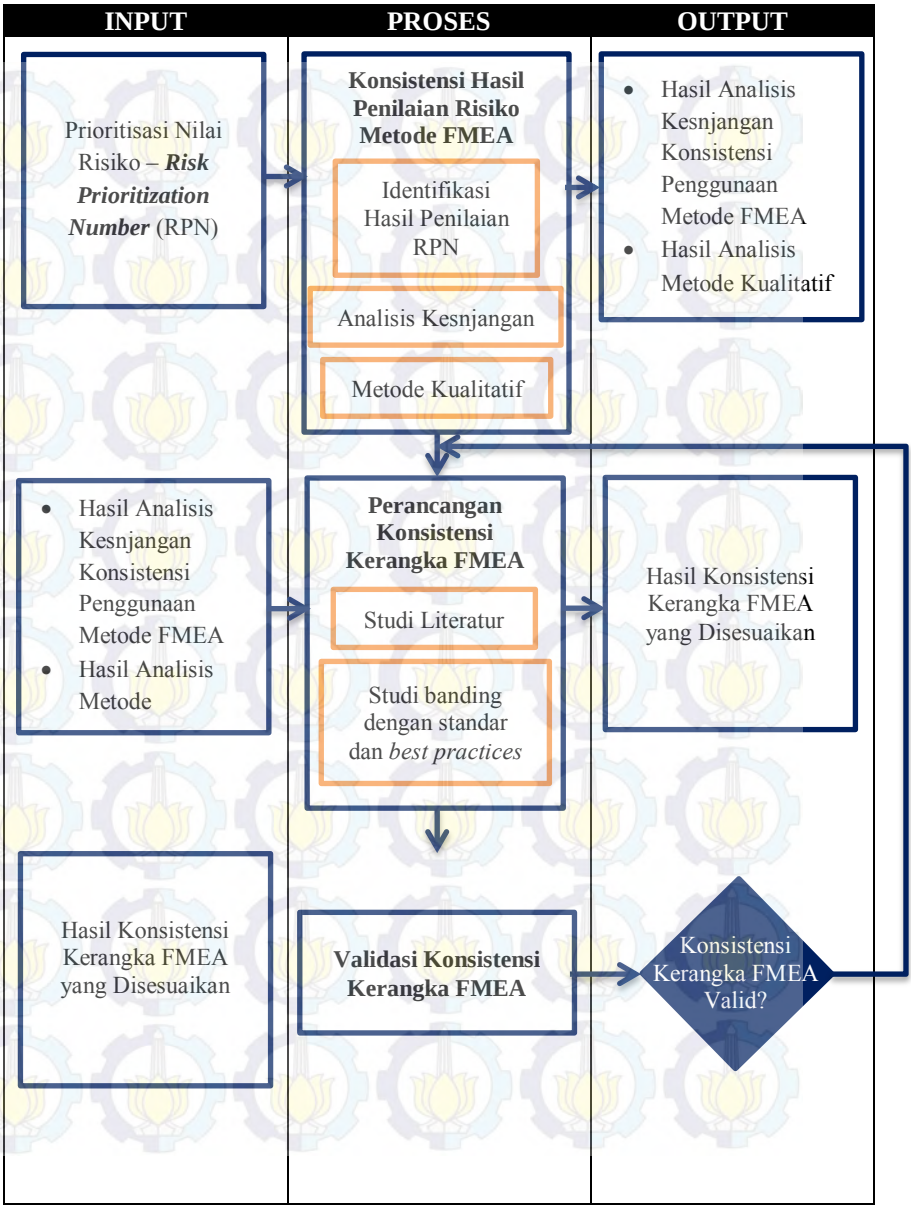
Gambar 3.1.1. Metode Konsep Pengerjaan (Sumber: Peneliti, 2014)

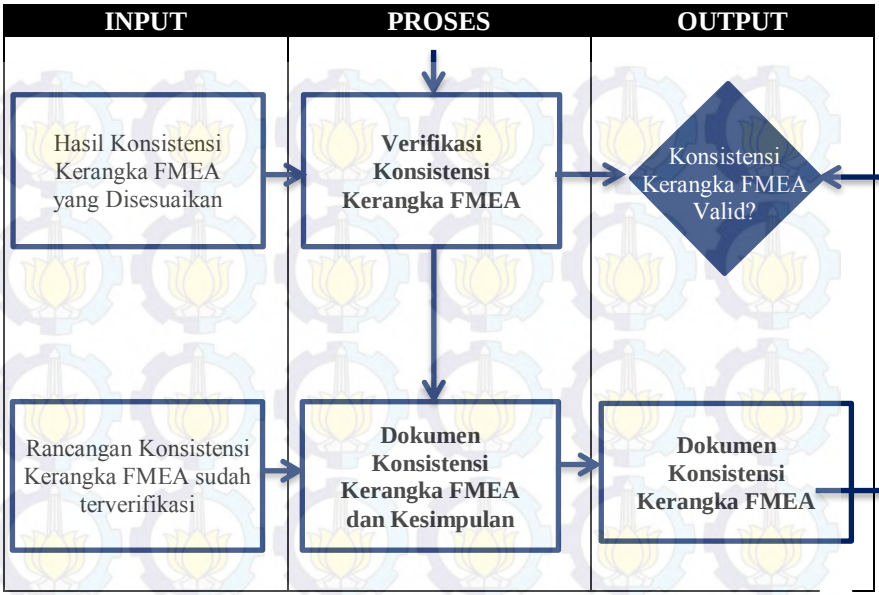
3.2. Metode Pengerjaan

Metode detail pengerjaan tugas akhir:

Tabel 3.1.1. Tabel Metode Pengerjaan (Sumber: Peneliti, 2014)




INPUT
PROSES
OUTPUT
Prioritisasi Nilai Risiko – *Risk Prioritization Number* (RPN)
Konsistensi Hasil Penilaian Risiko Metode FMEA
Identifikasi Hasil Penilaian RPN
Analisis Kesnjangan
Metode Kualitatif
Hasil Analisis Kesnjangan Konsistensi Penggunaan Metode FMEA
Hasil Analisis Metode Kualitatif
Hasil Analisis Kesnjangan Konsistensi Penggunaan Metode FMEA
Hasil Analisis Metode
Perancangan Konsistensi Kerangka FMEA
Studi Literatur
Studi banding dengan standar dan *best practices*
Hasil Konsistensi Kerangka FMEA yang Disesuaikan
Hasil Konsistensi Kerangka FMEA yang Disesuaikan
Validasi Konsistensi Kerangka FMEA
Konsistensi Kerangka FMEA Valid?



3.2.1. Identifikasi Permasalahan

Tahapan identifikasi permasalah untuk melakukan proses awal dalam pembuatan tugas akhir dengan tujuan menemukan permasalahan yang ada dalam melakukan identifikasi risiko penggunaan teknologi informasi yang ada pada perusahaan XYZ yang disesuaikan dengan kebijakan manajemen risiko yang telah diatur oleh perusahaan XYZ dan disesuaikam oleh Peraturan Bank Indonesia (PBI) Nomor 11/25/PBI/2009 mengenai Penerapan Manajemen Risiko Bagi Bank Umum.

Proses identifikasi permasalahan dilakukan dengan cara melakukan studi literatur sebagai bahan referensi dalam melakukan penelitian. Studi literatur yang digunakan berasal dari sumber buku, jurnal, dan karya tulis publikasi. Pada tahapan ini, dihasilkan rumusan masalah dari latar belakang permasalahan yang akan diangkat untuk memulai melakukan penelitian tugas akhir.

3.2.2. Pengumpulan Data

Pada tahapan pengumpulan data, dilakukan pengumpulan data dengan cara mengumpulkan data informasi, teori konsep dasar, dan kebutuhan data yang diperlukan serta melakukan wawancara dan observasi.

Pada tahapan ini, dilakukan penelitian untuk mempelajari prosedur, kebijakan, dan laporan tahunan perusahaan untuk membantu menyelesaikan permasalahan yang telah diangkat pada perumusan masalah. Metode yang dilakukan dalam melakukan pengumpulan data :

3.2.2.1. Wawancara terstruktur dan tidak terstruktur

Wawancara terstruktur akan dilakukan untuk menggali data dan informasi yang dilakukan pada Manajer Operasional Bank XYZ.

Wawancara tidak terstruktur dilakukan untuk menggali data dan informasi pada karyawan dibagian Teller Perusahaan XYZ yang mengjadi sampel penelitian yang dilakukan oleh dua tim berbeda dalam melakukan penilaian risiko menggunakan metode FMEA.

3.2.2.2. Observasi Peneliti

Observasi peneliti dilakukan untuk mengumpulkan data dan melakukan analisis risiko. Pada tahapan identifikasi risiko, diperlukan pengamatan secara langsung untuk dapat mengidentifikasikan dengan tepat mengenai risiko pada penerapan teknologi informasi.

Observasi dilakukan juga untuk mengamati kinerja karyawan pada bagian Teller dalam menerapkan teknologi informasi yang digunakan.

3.2.2.3. Mempelajari Dokumen Perusahaan

Pada tahapan mempelajari dokumen perusahaan dilakukan untuk mempelajari kebijakan, prosedur, dan laporan tahunan yang menjadi salah satu usaha yang

dilakukan untuk mendapatkan data dan informasi yang dibutuhkan. Hasil yang didapatkan untuk melakukan pengolahan informasi pada tahapan selanjutnya dalam melakukan analisis manajemen risiko.

3.2.3. Pengolahan Data

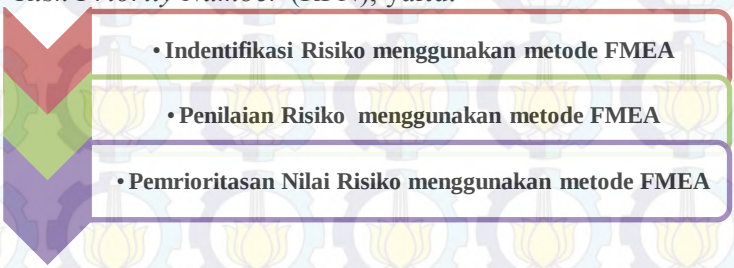
Pengolahan Data berdasarkan informasi proses bisnis, dampak dan risiko dalam proses bisnis perusahaan, maka proses selanjutnya adalah mengolah data dan informasi yang telah dimiliki. Terdapat dua bagian dalam proses ini yaitu melakukan analisis risiko pada daftar aset kritis dan analisis risiko.

3.2.3.1. Analisis Risiko Daftar Aset Kritis

Analisis risiko pada data aset kritis perusahaan untuk melakukan analisis penyebab dan dampak dari risiko yang terjadi. Sehingga memudahkan melakukan analisis risiko pada tahapan selanjutnya dalam melakukan penilaian risiko.

3.2.3.2. Analisis Risiko

Analisis Risiko menggunakan metode FMEA dengan tahapan melakukan identifikasi risiko, penilian risiko berdasarkan *severity, occurency*, dan *detection*, kemudian melakukan pemrioirtasan nilai risiko dengan *Risk Priority Number* (RPN), yaitu:



Gambar 3.2.3.2.1. Tahapan penilian risiko menggunakan metode FMEA (Sumber: FMEA)

1. ***Identifikasi risiko menggunakan metode FMEA***

   Identifikasi risiko menggunakan metode FMEA bertujuan untuk melakukan analisis terhadap risiko yang ada pada aset teknologi informasi yang ada pada perusahaan.

2. ***Pengukuran nilai risiko menggunakan metode FMEA***

   Pengukuran nilai risiko bertujuan untuk memberikan nilai pada setiap risiko berdasarkan nilai *severity*, *occurence*, dan *detection*.

3. ***Pemrioritasan nilai risiko menggunakan metode FMEA***

   Setelah melakukan penilaian pada setiap risiko, kemudian dilakukan pemrioritasan risiko menggunakan metode *Risk Prioritation Number* (RPN) yang ada pada FMEA.

3.2.4. Konsistensi Hasil Penilaian Risiko

Tahapan analisi konsistensi hasil penilaian risiko untuk melihat konsistensi penilaian risiko yang dilakukan menggunakan metode FMEA oleh dua tim yang berbeda, apakah sudah konsisten atau belum. Caranya dengan melakukan identifikasi hasil penilaian RPN pada dua sampel yang berbeda dan melakukan analisis kesenjangan.

3.2.4.1. Identifikasi Hasil Penilaian RPN

Pada identifikasi hasil penilian RPN untuk melakukan identifikasi apakah hasil penilian risiko pada dua sampe yang berbeda menghasilkan data yang sama atau tidak. Identifikasi dilakukan dengan cara melihat proses apa saja yang terjadi sehingga penggunaan metode FMEA menghasilkan data risiko yang konsisten walaupun diterapkan oleh dua tim yang berbeda.

3.2.4.2. Analisis Kesenjangan

Analisis kesenjangan dilakukan untuk melihat perbedaan yang terjadi antara penilian yang dilakukan oleh dua tim yang berbeda. Sehingga analisis kesenjangan yang dilakukan mengahasilkan kesimpulan yang didapatkan untuk mengidentifikasi konsistensi penggunaan metode FMEA dalam melakukan penilaian risiko.

3.2.5. Perancangan Kerangka FMEA yang Disesuaikan

Perancangan kerangka FMEA yang disesuaikan, dilakukan berdasarkan hasil yang didapatkan dari analisis kesenjangan pada konsistensi penggunaan metode FMEA dalam melakukan menajemen risiko. Dan perancangan modifikasi ini dilakukan berdasarkan studi literatur dan studi banding dengan standar serta best practice yang ada, untuk menghasilkan rekomendasi pembuatan kerangka FMEA yang disesuikan dengan kondisi perusahaan XYZ.

3.2.6. Validasi Kerangka FMEA yang Disesuaikan

Validasi kerangka FMEA yang Disesuaikan berdasarkan hasil yang telah dilakukan dengan melakukan penelitian menggunakan analisis kesenjangan dan penelitian kualitatif pada penggunaan teknologi informasi pada teller Bank XYZ. Apakah hasil yang diperoleh dari penilitian analisis kesenjangan dan kualitatif telah sesuai dengan rancangan Kerangka FMEA yang Disesuaikan dalam melakukan penilaian risiko untuk menghasilkan penilaiann risiko yang konsisten jika digunakan oleh tim yang berbeda dalam melakukan penilaian risiko.

3.2.7. Verifikasi Kerangka FMEA yang Disesuaikan

Verifikasi kerangka FMEA yang Disesuikan didukung dengan melakukan konfirmasi pada perusahaan Bank XYZ terkait pembuatan kerangka baru ini untuk melakukan penilian risiko dalam menghasilkan penilaian yang konsisten apakah telah sesuai dengan kebijakan dan prosedur yang telah ditetapkan oleh perusahaan Bank XYZ dan ketetapan dari Bank Indonesia.

3.2.8. Hasil Kerangka FMEA yang Disesuaikan

Hasil modifikasi kerangka FMEA yang telah dilakukan validasi dan verifikasi akan dilakukan pendokumentasian menjadi laporan tugas akhir secara keseluruhan.

BAB IV
PENILAIAN RISIKO DAN ANALISIS KESENJANGAN

Bab ini menjelaskan managemen risiko teknologi informasi pada perusahaan perbankan dengan melakukan penilaian risiko dengan menggunakan metode FMEA. Hasil penilaian risiko terkait hasil konsistensi, dilakukan pengujian menggunakan analisis kesenjangan dan menggunakan metode kualitatif untuk mendukung formulasi pembuatan Kerangka FMEA yang Disesuaikan.

4.1. Analasis Proses Bisnis Teller Bank XYZ

Hasil analisis yang dilakukan dari wawancara di Bank XYZ mengenai proses Bisnis pada Teller Bank XYZ, yaitu:

1. Teller menanyakan keperluan transaksi yang akan dibuat oleh nasabah.
2. Melakukan proses validasi kepemilikan informasi nasabah untuk melakukan proses transaksi.
3. Teller melakukan proses transaksi nasabah ke dalam sistem yang telah disediakan yaitu menggunakan sistem F@st yang berfungsi untuk mencatat transaksi.
4. Teller menggunakan SVS untuk melakukan verifikasi tanda tangan yang dimiliki oleh nasabah.
5. Data transaksi yang telah dilakukan oleh teller dan nasabah akan dicatat pada sistem HOST.
6. Jika teller belum berhasil melakukan verifikasi transaksi karena melebihi limit harian yang dapat diakses oleh tiap teller, maka ada wewenang dari pihak Pimpinan atau Supervisor untuk memberikan validasi akses transaksi.

7. Data transaksi yang tersimpan mulai open branch hingga *close branch* akan direkap dan divalidasi ulang oleh pimpinan atau Supervisor untuk memastikan valid atau tidaknya jumlah transaksi yang dilakukan.

Penjelasan lebih lengkap mengenai tugas pokok dan fungsi pada sistem teller adalah sebagai berikut:

1. F@st adalah sistem yang digunakan untuk melakukan transaksi pada bagian teller meliputi proses setoran dan penarikan tunai (*overbooking* – sesama rekening Bank) dan penarikan non tunai, melalui kliring (setoran menggunakan warkat Bank lain), transfer tunai maupun non tunai, penerimaan *collection* (warkat Bank luar negeri), jual beli valuta asing, pembayaran kartu kredit. Sistem ini dibuat sendiri oleh bagian TI pada Bank XYZ.
2. Host adalah sistem yang digunakan untuk penyimpanan data nasabah yang terdapat di bagian server Bank XYZ. Sehingga di dalam sistem ini berisikan seluruh data diri dan transaksi nasabah. Transaksi yang dilakukan oleh nasabah yang menggunakan sistem F@st, seluruh datanya akan disimpan ke dalam server menggunakan sistem Host.
3. SVS (Signature Verification System) adalah sistem yang digunakan untuk melakukan verifikasi tanda tangan nasabah yang valid. Sistem ini berjalan ketika proses transaksi dengan sistem F@st dan dilakukan verifikasi tanda tangan melalui sistem ini untuk selanjutnya diproses.

4.2. Identifikasi Aset Kritis Teller Bank XYZ

Dari hasil analisis yang dilakukan sesuai dengan metodologi maka dilakukan proses identifikasi aset kritis diperoleh bahwa proses bisnis di bagian teller telah diidentifikasikan dari aset secara umum kemudian ditentukan aset kritis atau pentingnya berdasarkan setiap sistem yang digunakan di bagian *teller*.

a. Sistem F@st

Pengkategorian aset kritis berdasarkan Informasi, Hardware, Software, dan People pada F@st beserta penjelasan penggunaan F@st:

Tabel 4.2.1. Identifikasi Sistem F@st (Sumber: Peneliti, 2014)

No	Kategori Aset	Aset Kritis	Deskripsi
1	Informasi	Data transaksi setoran dan penarikan tunai (*overbooking* – sesama rekening Bank) dan penarikan non tunai, melalui kliring (setoran menggunakan warkat Bank lain), Data transfer tunai maupun non tunai, Data penerimaan collection (warkat Bank luar negeri), Data jual beli valuta asing, Data pembayaran kartu kredit. Password user *teller*, Informasi diri nasabah	Data transaksi ini digunakan oleh nasabah untuk melakukan proses transaksi di bagian *teller*.
2	Hardware	Server	Digunakan dalam menyimpan data transaksi pada sistem ini yang ada pada bagian teller Bank XYZ
		Komputer	Digunakan untuk membantu teller dalam melakukan proses transaksi nasabah seperti memasukkan data,

No	Kategori Aset	Aset Kritis	Deskripsi
			mengirimkan data dan mengolah data.
		Jaringan intranet dan internet, Hub, Router	Digunakan untuk mendukung jaringan yang digunakan dalam sistem agar dapat melakukan komunikasi dan proses transaksi
		Hardware pendukung proses transaksi di *teller* yang meliputi : Printer, Alat Penghitung Uang, Lampu pengidentifikasi uang palsu atau asli	Digunakan sebagai pendukung dalam proses transaksi pada sistem seperti penghitung uang nasabah, pengidentifikasi uang palsu dan asli
3	Software	Kapersky	Digunakan sebagai software untuk mendukung antivirus
		Sistem operasi Linux Ubuntu dan Windows, Arcansas	Digunakan sebagai software untuk mendukung sistem ini di bagian sistem operasi
4	People	Teller, Pimpinan Cabang, Tim TI	Merupakan pihak-pihak yang berwenang dalam penggunaan sistem ini

b. Sistem Host

Pengkategorian aset kritis berdasarkan Informasi, Hardware, Software, dan People pada Host beserta penjelasan penggunaan Host:

Tabel 4.2.2. Identifikasi Sistem Host (Sumber: Peneliti, 2014)

No	Kategori Aset	Aset Kritis	Deskripsi
1	Informasi	Data transaksi setoran dan penarikan tunai (*overbooking* – sesama rekening Bank) dan penarikan non tunai, melalui kliring (setoran menggunakan warkat Bank	Data transaksi ini digunakan oleh nasabah untuk melakukan proses penyimpanan data transaksi di bagian *teller*.

No	Kategori Aset	Aset Kritis	Deskripsi
		lain), Data transfer tunai maupun non tunai, Data penerimaan collection (warkat Bank luar negeri), Data jual beli valuta asing, Data pembayaran kartu kredit. Password user *teller*, Informasi diri nasabah	
2	Hardware	Server	Digunakan dalam menyimpan data transaksi pada sistem ini yang ada pada bagian teller Bank XYZ
		Komputer	Digunakan untuk membantu teller dalam melakukan proses transaksi nasabah seperti memasukkan data, mengirimkan data dan mengolah data.
		Jaringan intranet dan internet, Hub, Router	Digunakan untuk mendukung jaringan yang digunakan dalam sistem agar dapat melakukan komunikasi dan proses transaksi
3	Software	Kapersky	Digunakan sebagai software untuk mendukung sistem ini, mulai dari antivirus
		Sistem operasi Linux Ubuntu dan Windows, Arcansas	Digunakan sebagai software untuk mendukung sistem ini berdasarkan sistem operasi
4	People	Teller, Pimpinan Cabang, Tim TI	Merupakan pihak-pihak yang berwenang dalam penggunaan sistem ini

c. Sistem SVS

Pengkategorian aset kritis berdasarkan Informasi, Hardware, Software, dan People pada SVS beserta penjelasan penggunaan SVS:

Tabel 4.2.3. Identifikasi Sistem SVS (Sumber: Peneliti, 2014)

No	Kategori Aset	Aset Kritis	Deskripsi
1	Informasi	Data transaksi setoran dan penarikan tunai (*overbooking* – sesama rekening Bank) dan penarikan non tunai, melalui kliring (setoran menggunakan warkat Bank lain), Data transfer tunai maupun non tunai, Data penerimaan collection (warkat Bank luar negeri), Data jual beli valuta asing, Data pembayaran kartu kredit. Password user *teller*, Informasi diri nasabah	Data transaksi ini digunakan oleh nasabah untuk melakukan proses validasi data transaksi di bagian *teller*.
2		Server	Digunakan dalam menyimpan data transaksi pada sistem ini yang ada pada bagian teller Bank XYZ
		Komputer	Digunakan untuk membantu teller dalam melakukan proses transaksi nasabah seperti memasukkan data, validasi data.
		Jaringan intranet dan internet, Hub, Router	Digunakan untuk mendukung jaringan yang digunakan dalam sistem agar dapat melakukan komunikasi dan proses transaksi
		Scanner	Digunakan untuk melakukan scanning

No	Kategori Aset	Aset Kritis	Deskripsi
	Hardware		
3	Software	Kapersky	Digunakan sebagai software untuk mendukung sistem ini, mulai dari antivirus
		Sistem operasi Linux Ubuntu dan Windows, Arcansas	Digunakan sebagai software untuk mendukung sistem ini di bagian sistem operasi
4	People	Teller, Pimpinan Cabang, Tim TI	Merupakan pihak-pihak yang berwenang dalam penggunaan sistem ini

4.3. Membangun Aset Berbasis Ancaman

Identifikasi ancaman pada aset TI yang diterapkan pada Teller Bank XYZ:

4.3.1. Profil Kebutuhan Keamanan untuk Aset kritis

Berdasarkan dengan metodologi mengenai proses ini dan mengacu pada tiga elemen aspek keamanan yaitu, ketersediaan, integritas, dan kerahasiaan yang dijelaskan pada tabel dibawah ini :

a. Sistem F@st

Profil kebutuhan keamanan pada F@st terkait dengan ketersediaan, integritas, dan kerahasian aset kritis.

Tabel 4.3.1.1. Profil Kebutuhan Keamanan F@st (Sumber: Peneliti, 2014)

Aset Kritis	Ketersediaan	Kerahasiaan	Integritas
Informasi : Data transaksi setoran dan penarikan tunai dan penarikan non tunai, melalui kliring, Data	Informasi harus ada selama jam kerja	Tidak boleh digunakan oleh orang yang tidak memiliki hak otorisasi	Tidak boleh ada yang bisa merubah dan menghapus isi data kecuali orang yang berhak

Aset Kritis	Ketersediaan	Kerahasiaan	Integritas
transfer tunai maupun non tunai, Data penerimaan collection, Data jual beli valuta asing, Data pembayaran kartu kredit. Password user *teller*, Informasi diri nasabah			
Hardware			
Server	Hardware harus bisa digunakan secara optimal selama 24 jam 7 hari	Harus dijaga keberadaannya dari orang yang tidak berhak baik secara fisik maupun logika.	Harus dijamin kredibilitas dan kepastian mesin terhadap pengguna yang berhak
Komputer	Sistem harus bisa berfungsi selama jam kerja	Pihak yang login ke sistem harus dilindungi kerahasiaan autentikasinya	Tidak boleh ada yang bisa login ke sistem kecuali orang yang berhak
Intranet dan Internet, Hub, dan Router	Sistem harus bisa berfungsi selama jam kerja	Pihak yang login ke sistem harus dilindungi kerahasiaan autentikasinya	Tidak boleh ada yang bisa login ke sistem kecuali orang yang berhak
Hardware pendukung proses transaksi di *teller* yang meliputi : Printer, Alat Penghitung Uang, Lampu pengidentifikasi uang palsu atau asli.	Sistem harus bisa berfungsi selama jam kerja	Dipergunakan seoptimal mungkin oleh pihak yang berwenang.	Hanya orang yang berkepentingan saja yang dapat mengakses.
Software	Resource software harus	Akses admin software yang	Software tidak dapat digunakan

Aset Kritis	Ketersediaan	Kerahasiaan	Integritas
	tersedia jika akan digunakan	berhak harus dijaga kerahasiaannya	dan dimodifikasi oleh orang yang tidak berhak
People	Tim TI harus siap melayani ketersediaan sistem 24 jam 7 hari	User dan password autentikasi dijaga kerahasiaannya	Administrator yang kredibel yang boleh melakukan konfigurasi aset kritis

b. Sistem Host

Profil kebutuhan keamanan pada Host terkait dengan ketersediaan, integritas, dan kerahasian aset kritis.

Tabel 4.3.1.2. Profil Kebutuhan Keamanan Host (Sumber: Peneliti, 2014)

Aset Kritis	Ketersediaan	Kerahasiaan	Integritas
Informasi	Informasi harus ada selama jam kerja	Tidak boleh digunakan oleh orang yang tidak memiliki hak otorisasi	Tidak boleh ada yang bisa merubah dan menghapus isi data kecuali orang yang berhak
Hardware			
Server	Hardware harus bisa digunakan secara optimal selama 24 jam 7 hari	Harus dijaga keberadaannya dari orang yang tidak berhak baik secara fisik maupun logika.	Harus dijamin kredibilitas dan kepastian mesin terhadap pengguna yang berhak
Komputer, intranet dan internet, hub, router	Sistem harus bisa berfungsi selama jam kerja.	Pihak yang login ke sistem harus dilindungi kerahasiaan autentikasinya	Tidak boleh ada yang bisa login ke sistem kecuali orang yang berhak.
Software	Resource software harus tersedia jika akan digunakan	Akses admin software yang berhak harus dijaga kerahasiaannya	Software tidak dapat digunakan dan dimodifikasi oleh orang yang tidak berhak

Aset Kritis	Ketersediaan	Kerahasiaan	Integritas
People	Tim TI harus siap melayani ketersediaan sistem 24 jam 7 hari	User dan password autentikasi dijaga kerahasiaannya	Administrator yang kredibel yang boleh melakukan konfigurasi aset kritis

c. **Sistem SVS**

Profil kebutuhan keamanan pada SVS terkait dengan ketersediaan, integritas, dan kerahasian aset kritis.

Tabel 4.3.1.3. Profil Kebutuhan Keamanan SVS (Sumber: Peneliti, 2014)

Aset Kritis	Ketersediaan	Kerahasiaan	Integritas
Informasi	Informasi harus ada selama jam kerja	Tidak boleh digunakan oleh orang yang tidak memiliki hak otorisasi	Tidak boleh ada yang bisa merubah dan menghapus isi data kecuali orang yang berhak
Hardware			
Server	Hardware harus bisa digunakan secara optimal selama 24 jam 7 hari	Harus dijaga keberadaannya dari orang yang tidak berhak baik secara fisik maupun logika.	Harus dijamin kredibilitas dan kepastian mesin terhadap pengguna yang berhak
Komputer, intranet dan internet, hub, router	Sistem harus bisa berfungsi selama jam kerja.	Pihak yang login ke sistem harus dilindungi kerahasiaan autentikasinya	Tidak boleh ada yang bisa login ke sistem kecuali orang yang berhak.
Scanner	Sistem harus bisa berfungsi selama jam kerja.	Dipergunakan seoptimal mungkin oleh pihak yang berwenang.	Hanya orang yang berkepentingan saja yang dapat mengakses.
Software	Resource software harus	Akses admin software yang	Software tidak dapat digunakan

Aset Kritis	Ketersediaan	Kerahasiaan	Integritas
	tersedia jika akan digunakan	berhak harus dijaga kerahasiaannya	dan dimodifikasi oleh orang yang tidak berhak
People	Tim TI harus siap melayani ketersediaan sistem 24 jam 7 hari	User dan password autentikasi dijaga kerahasiaannya	Administrator yang kredibel yang boleh melakukan konfigurasi aset kritis

4.3.2. Ancaman terhadap Aset Kritis

Dari aset kritis yang ada di bagian *teller* Bank XYZ, maka dapat dilihat ancaman dari aset kritis sebagai berikut:

a. Sistem F@st

Ancaman yang mungkin terjadi yang berasal dari internal dan eksternal pada penggunaan F@st.

Tabel 4.3.2.1. Ancaman pada Penggunaan F@st (Sumber: Peneliti, 2014)

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
Informasi	Data transaksi setoran dan penarikan tunai dan penarikan non tunai, melalui kliring, Data transfer tunai maupun non tunai, Data penerimaan collection, Data jual beli valuta asing, Data pembayaran kartu kredit. Password user *teller*, Informasi diri nasabah	• Pembobolan informasi terhadap sistem dengan melakukan pembagian password user teller • Ketidaksesuaian proses transaksi (seperti tidak samanya antara debit dan kredit) akibat kesalahan memasukkan masukkan nilai	Adanya bencana alam di area Bank XYZ yang menyebabkan kerusakan informasi
Hardware	Server	• Kerusakan server	• Adanya bencana

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
		akibat adanya kebocoran • Kesalahan dalam konfigurasi server sehingga tidak dapat digunakan • Kerusakan server akibat adanya runtuhan yang mengenai server	alam di area Bank XYZ yang menyebabkan kerusakan pada server • Terjadinya kebakaran akibat kelalaian
	Komputer	• Kesalahan dalam konfigurasi komputer sehingga tidak dapat digunakan • Adanya virus yang menyerang • Lisensi software yang digunakan sudah melebihi batas waktu	• Terjadinya kebakaran akibat kelalaian • Adanya pencurian komputer
	Intranet dan Internet, Hub, dan Router	• Penyalahgunaan penggunaan oleh karyawan yang tidak sesuai dengan proses bisnis • Kesalahan dalam melakukan konfigurasi • Kerusakan akibat *maintenance* yang tidak rutin	• Adanya *hacker* yang dapat masuk pada sistem melalui celah penggunaan internet
	Hardware pendukung proses transaksi di *teller* yang meliputi:	• Kesalahan penggunaan prosedur	Adanya bencana alam di area Bank XYZ sehingga menimbulkan

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
	Printer, Alat Penghitung Uang, Lampu pengidentifikasi uang palsu atau asli.		kerusakan pada hardware
Software	Kapersky	• Telat melakukan perpanjangan lisensi	Adanya bencana alam menyebabkan rusaknya software
	Sistem operasi Linux Ubuntu dan Windows, Arcansas	• Salah melakukan prosedur penginstallan • Telat melakukan perpanjangan lisensi	Adanya bencana alam menyebabkan rusaknya software
		Adanya bencana alam menyebabkan rusaknya software	Adanya bencana alam yang menyebabkan kerusakan sistem
People	Teller, Pimpinan Cabang, Tim TI	Pengetahuan karyawan yang menurun	• Kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem

b. Sistem Host

Ancaman yang mungkin terjadi yang berasal dari internal dan eksternal pada penggunaan Host.

Tabel 4.3.2.1. Ancaman pada Penggunaan Host (Sumber: Peneliti, 2014)

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
Informasi	Data transaksi setoran dan penarikan tunai dan penarikan non tunai, melalui kliring, Data transfer tunai maupun non tunai, Data penerimaan collection, Data jual beli valuta asing, Data pembayaran kartu kredit. Password user *teller*, Informasi diri nasabah	• Pembobolan informasi terhadap sistem dengan melakukan pembagian password user teller • Ketidaksesuaian proses transaksi (seperti tidak samanya antara debit dan kredit) akibat kesalahan memasukkan masukkan nilai	Adanya bencana alam di area Bank XYZ yang menyebabkan kerusakan informasi
Hardware	Server	• Kerusakan server akibat adanya kebocoran • Kesalahan dalam konfigurasi server sehingga tidak dapat digunakan • Kerusakan server akibat adanya runtuhan yang mengenai server	• Adanya bencana alam di area Bank XYZ yang menyebabkan kerusakan pada server • Terjadinya kebakaran akibat kelalaian
	Komputer	• Kesalahan dalam konfigurasi komputer sehingga tidak dapat digunakan • Adanya virus yang	• Terjadinya kebakaran akibat kelalaian • Adanya pencurian

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
		menyerang • Lisensi software yang digunakan sudah melebihi batas waktu	komputer
	Intranet dan Internet, Hub, dan Router	• Penyalahgunaan penggunaan oleh karyawan yang tidak sesuai dengan proses bisnis • Kesalahan dalam melakukan konfigurasi • Kerusakan akibat *maintenance* yang tidak rutin	• Adanya *hacker* yang dapat masuk pada sistem melalui celah penggunaan internet
Software	Kapersky	• Telat melakukan perpanjangan lisensi	• Adanya bencana alam yang menyebabkan rusaknya software
	Sistem operasi Linux Ubuntu dan Windows, Arcansas	• Kerusakan akibat *maintenance* yang tidak rutin • Penggunaan yang tidak sesuai dengan prosedur • Telat melakukan perpanjangan lisensi	• Adanya bencana alam yang dapat menyebabkan rusaknya software
	Sistem Host	Salah melakukan prosedur penggunaan sistem	Adanya bencana alam yang menyebabkan kerusakan sistem

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
People	Teller, Pimpinan Cabang, Tim TI	Pengetahuan karyawan yang menurun	Kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem

c. Sistem SVS

Ancaman yang mungkin terjadi yang berasal dari internal dan eksternal pada penggunaan SVS.

Tabel 4.3.2.2. Ancaman pada Penggunaan SVS (Sumber: Peneliti, 2014)

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
Informasi	Data transaksi setoran dan penarikan tunai dan penarikan non tunai, melalui kliring, Data transfer tunai maupun non tunai, Data penerimaan collection, Data jual beli valuta asing, Data pembayaran kartu kredit. Password user *teller*, Informasi diri nasabah	• Pembobolan informasi terhadap sistem dengan melakukan pembagian password user teller • Ketidaksesuaian proses transaksi (seperti tidak samanya antara debit dan kredit) akibat kesalahan memasukkan masukkan nilai	Adanya bencana alam di area Bank XYZ yang menyebabkan kerusakan informasi
Hardware	Server	• Kerusakan server akibat adanya kebocoran • Kesalahan dalam konfigurasi server sehingga tidak	• Adanya bencana alam di area Bank XYZ yang menyebabkan kerusakan pada server

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
		dapat digunakan • Kerusakan server akibat adanya runtuhan yang mengenai server	• Terjadinya kebakaran akibat kelalaian
	Komputer	• Kesalahan dalam konfigurasi komputer sehingga tidak dapat digunakan • Adanya virus yang menyerang • Lisensi software yang digunakan sudah melebihi batas waktu	• Terjadinya kebakaran akibat kelalaian • Adanya pencurian komputer
	Intranet dan Internet, Hub, dan Router	• Penyalahgunaan penggunaan oleh karyawan yang tidak sesuai dengan proses bisnis • Kesalahan dalam melakukan konfigurasi • Kerusakan akibat *maintenance* yang tidak rutin	• Adanya *hacker* yang dapat masuk pada sistem melalui celah penggunaan internet
	Hardware pendukung proses transaksi di *teller* yang meliputi: *scanner*	• Kesalahan penggunaan prosedur	Adanya bencana alam di area Bank XYZ sehingga menimbulkan kerusakan pada hardware

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
Software	Kapersky	Telat melakukan perpanjangan lisensi	Adanya bencana alam yang menyebabkan rusaknya software
	Sistem operasi Linux Ubuntu dan Windows, Arcansas	Telat melakukan perpanjangan lisensi	Adanya bencana alam yang menyebabkan rusaknya software
People	Teller, Pimpinan Cabang, Tim TI	Pengetahuan karyawan yang menurun	• Kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem

4.3.3. *Current Security Practices*

Dalam hal ini berisikan informasi keamanan yang telah diterapkan oleh bagian teller Bank XYZ. Sehingga hal tersebut dapat dilihat sebagai berikut:

Tabel 4.3.3.1. Current Security Practice pada teller Bank XYZ (Sumber: Peneliti, 2014)

Current Security Practices	Pihak yang bertanggung jawab
Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali. Hal ini digunakan untuk menjaga keamanan yang ada pada sistem, agar mengurangi gangguan sistem yang berjalan.	Tim TI
Melakukan pengecekan terhadap sistem	Pimpinan Cabang

transaksi setiap hari yang dilakukan pada close brand (pukul 15.00 WIB) dan open brand (pukul 08.00 WIB). Hal ini dilakukan untuk mengantisipasi adanya pelanggaran, kesalahan dalam proses transaksi	
Adanya SOP terkait pengembangan sumber daya karyawan.	Pimpinan Cabang
Adanya software untuk anti virus dan pendeteksi IP yang tidak terdaftar. Hal ini dilakukan untuk mengantisipasi adanya kerusakan sistem, dan menjaga kerahasiaan sistem serta data transaksi yang ada di perusahaan.	Tim TI
Tata letak aset diletakkan pada posisi yang sesuai dengan standar untuk mengantisipasi bencana alam (banjir dan gempa)	Tim TI
Adanya SOP terkait sharing password karyawan, sehingga dapat meminimalisir terjadinya penyebaran informasi	Pimpinan Cabang

4.3.4. *Current Organizational Vulnerabilities*

Dalam hal ini bagian teller Bank XYZ melakukan identifikasi kelemahan dari pihak organisasi yang dijelaskan sebagai berikut :

- Apabila terjadi bencana alam (banjir) pada wilayah Jawa Barat yaitu pada kota Bogor dan Jakarta, maka Back up data akan berisiko tidak terselamatkan. Karena kedua lokasi memiliki potensi bencana alam yang tinggi.
- Server pusat ada di Jakarta , sehingga apabila bagian Jakarta mengalami masalah seperti down maka dapat mempengaruhi jaringan pengiriman data di Bank XYZ.

- Prosedur maintenance hardware pendukung dilakukan setiap bulan. Sehingga apabila kerusakan terjadi pada hari tertentu belum terdapat prosedur yang mendukung hal tersebut.
    - Tidak adanya dokumen pendukung terkait penanganan kerusakan software.
    - Tidak adanya prosedur penginstallan sistem operasi.
    - Tidak adanya prosedur penanganan kesalahan penggunaan aplikasi system.
    - Tidak adanya prosedur penanganan penurunan etika kerja karyawan terhadap keamanan system.
    - Pelatihan yang diikuti karyawan kurang yaitu dilakukan 2 bulan sekali

4.4. Identifikasi Kelemahan Infrastruktur

Pada pembahasan technical view menjelaskan identifikasi pada infrastruktur yang digunakan pada Teller Bank XYZ sebagai bagaian pendukung penggunaan aset TI.

4.4.1. Key Components

Key Components menjelaskan tentang penggunaan infrastruktur dan informasi yang ada pada Teller Bank XYZ sebagai bagian dari proteksi aset TI yang digunakan, yang dijelaskan sebagai berikut :

- Server di dalam cabang terdapat server dengan data akan langsung terhubung ke dalam server pusat di Jakarta.

- Jaringan, di dalam Bank XYZ menggunakan jaringan intranet dan internet.

4.4.2. Current Technology Vulnerabilities

Penerapan teknologi informasi pada Teller Bank XYZ yang masih memiliki kelemahan diantaranya:

Tabel 4.4.2.1. *Current Technology Vulnerabilities* (Sumber: Peneliti, 2014)

Key Components	*Vulnerabilities*
Server	Server pusat terletak di Bank XYZ, Jakarta dan back up server terletak di Bank XYZ Bogor. Sehingga ada kelemahan jika terjadi bencana atau kerusuhan di daerah Jawa Barat. Maka tidak ada back up lagi pada data.
Jaringan	Jika jaringan mati, belum ada back up sistem yang mampu mencatat transaksi yang terjadi pada teller. Sehingga teller harus menggunakan cara konvensional dalam melakukan pencatatan transaksi yang memungkinkan terjadinya ketidaksamaan data atau kelalaian.
Hardware Pendukung	Komponen penyusun hardware pendukung tidak asli
Software (Kapersky)	Software tidak dapat melakukan update secara otomatis
Software (Sistem Operasi)	Software tidak dapat mendeteksi aplikasi tidak berlisensi
Software (Aplikasi Sistem)	Software masih terdapat celah keamanan

4.5. Identifikasi dan Penilaian Risiko

Identifikasi dan Penilaian Risiko pada teller Bank XYZ dengan cara mengidentifikasi risiko yang ada, dan kemudian melakukan penilaian risiko pada setiap akibat yang mungkin terjadi, penyebab dari risiko, hingga cara melakukan control.

4.5.1. Analisis Nilai Risiko

Analisis risiko pada proses bisnis pada teller Bank XYZ menggunakan metode FMEA dengan memberikan penilaian berdasarkan *severity, occurency*, dan *detection* pada tiap risiko untuk menghasilkan Risk Priority Number (RPN).

Analisis risiko menggunakan metode FMEA pada penggunaan teknologi informasi pada teller Bank XYZ dilakukan oleh dua tim berbeda, yaitu tim A dan tim B. Dimana tim A terdiri dari dua mahasiswa yang baru saja mengambil mata kuliah managemen risiko, dan tim B yang terdiri dari mahasiswa dan narasumber yang bertanggung jawab terhadap penilaian risiko pada bagian operasional Bank XYZ. Maka hasil analisis risiko menggunakan metode FMEA yang dilakukan oleh dua tim, yaitu:

Hasil Analisis Risiko Tim A

Hasil analisis risiko yang dilakukan oleh Tim A pada teller Bank XYZ untuk menghasilkan *Risk Priority Number* (RPN) pada risiko dari hasil analisis yang dilakukan pada dampak yang akan terjadi pada risiko yang ditimbulkan (severity), kemungkinan risiko terjadi pada perusahaan (occurency), deteksi yang telah dilakukan oleh perusahaan terhadap risiko yang mungkin terjadi (detection). Tim A melakukan penilaian risiko menggunakan metode FMEA dilakukan oleh dua orang yang telah mempelajari penggunaan metode FMEA untuk melakukan manajemen risiko dan seorang narasumber, Manager Operation dari Bank XYZ.

Tabel 4.5.1.1. Hasil Analisis Risiko Tim A (Sumber: Peneliti, 2014)

Code	*Process Function (Step)*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
R1.1	Informasi	Pembobolan informasi	Penyebaran informasi perusahaan	7	Sharing password yang dilakukan oleh karyawan	2	Adanya SOP terkait sharing password karyawan	2	28
R1.2		Pembobolan informasi	Penyebaran informasi perusahaan	7	Sistem disadap oleh penyadap	2	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	2	28
R1.3		Pembobolan informasi	Kerugian finansial	7	Bencana alam	2	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	56

Code	*Process Function (Step)*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
R1.4		Kegagalan sistem transaksi	Penyebaran informasi perusahaan	6	Kesalahan dalam melakukan input transaksi	3	Pengecekkan terhadap sistem transaksi setiap hari	2	36
R1.5		Kegagalan sistem transaksi	Kerugian finansial	6	Bencana alam	3	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	72
R1.6		Kegagalan sistem transaksi	Kerugian finansial	6	Sistem mati dan tidak dapat diakses	2	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	4	48
R2.1	Hardware	Kerusakan server	Server tidak dapat digunakan	8	Kebocoran pada ruangan server	2	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	5	80
R2.2		Kerusakan server	Server tidak dapat digunakan	8	Kesalahan dalam konfigurasi	6	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	5	240
R2.3		Kerusakan server	Kerugian finansial	7	Keruntuhan bangunan	4	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan	4	112

Code	Process Function (Step)	Potential Failure Modes (process defects)	Potential Effect(s) of Failure	SEV	Potential Cause(s) of Failure	OCC	Current Process Controls	DET	RPN
							sekali		
R2.4		Kerusakan server	Kerugian finansial	8	Bencana alam	3	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	96
R2.5		Kerusakan server	Server tidak dapat digunakan	7	Terjadinya kerusakan pada komponen yang ada di server : kabel putus	4	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan	4	112
R2.6		Kerusakan komputer	Proses bisnis terhambat pada bagian teller seperti menimbulkan antrian	6	Adanya virus yang menyerang	2	Adanya software untuk anti virus	4	48
R2.7		Kerusakan komputer	Proses bisnis terhambat pada bagian teller seperti menimbulkan antrian	6	Lisensi software yang digunakan sudah melebihi batas waktu	5	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan	4	120
R2.8		Kerusakan komputer	Kerugian finansial	6	Bencana alam	5	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	120
R2.9		Kerusakan komputer	Kerugian finansial	6	Kebocoran pada ruangan komputer	3	Melakukan pengecekkan secara rutin terhadap	4	72

Code	Process Function (Step)	Potential Failure Modes (process defects)	Potential Effect(s) of Failure	SEV	Potential Cause(s) of Failure	OCC	Current Process Controls	DET	RPN
							keamanan sistem setiap bula		
R2.10		Kerusakan komputer	Kerugian finansial	5	Keruntuhan bangunan	2	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	5	50
R2.11		Kerusakan komputer	Proses bisnis terhambat pada bagian teller seperti menimbulkan antrian	5	Terjadinya kerusakan pada komponen yang ada pada komputer : monitor rusak,keyboard rusak dll	2	Melakukan pengecekan secara secara rutin terhadap keamanan sistem setiap bulan	4	40
R2.12		Kerusakan pada intranet, internet, hub dan router	Tidak dapat diakses secara rela time	5	Kesalahan dalam melakukan konfigurasi	2	Melakukan pengecekan secara secara rutin terhadap keamanan sistem setiap bulan	4	40
R2.13		Kerusakan pada intranet, internet, hub dan router	Proses bisnis terhambat pada bgian teller yaitu komunikasi di bagian teller tidak menjadi lancar	5	Maintenance yang tidak rutin	2	Melakukan pengecekan secara secara rutin terhadap keamanan sistem setiap bulan	4	40
R2.14		Kerusakan pada intranet, internet,	Proses bisnis terhambat pada bgian teller yaitu	6	Adanya hacker yang dapat masuk pada	3	Adanya pendeteksi IP yang tidak terdaftar	2	36

Code	Process Function (Step)	Potential Failure Modes (process defects)	Potential Effect(s) of Failure	SEV	Potential Cause(s) of Failure	OCC	Current Process Controls	DET	RPN
		hub dan router	komunikasi di bagian teller tidak menjadi lancar		sistem melalui celah pengggunaan internet				
R2.15		Kerusakan pada intranet, internet, hub dan router	Kerugian finansial	6	Bencana alam	3	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	72
R2.16		Kerusakan pada intranet, internet, hub dan router	Kerugian finansial	6	Keruntuhan bangunan	2	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	48
R2.17		Kerusakan pada intranet, internet, hub dan router	Teller Bank XYZ kembali menggunakan sistem konvensional	5	Terjadinya kerusakan pada hub dan router	4	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	4	80
R2.18		Kerusakan hardware pendukung	Proses bisnis terhambat yaitu menimbulkan antrian nasabah	5	Komponen penyusun hardware pendukung tidak asli	3	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	4	60
R2.19		Kerusakan hardware pendukung	Proses bisnis terhambat pada bagian teller seperti menimbulkan antrian	5	Prosedur maintenance hardware pendukung dilakukan setiap	3	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	4	60

Code	Process Function (Step)	Potential Failure Modes (process defects)	Potential Effect(s) of Failure	SEV	Potential Cause(s) of Failure	OCC	Current Process Controls	DET	RPN
					bulan				
R2.20		Kerusakan hardware pendukung	Kerugian finansial	5	Adanya bencana alam di area Bank XYZ	6	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	120
R3.1	Software	Kerusakan kapersky	Kerugian finansial	6	Bencana alam	4	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	2	48
R3.2		Kerusakan kapersky	Proses bisnis terhambat pada bagian teller yaitu sistem menjadi terkena virus	6	Software tidak dapat melakukan update secara otomatis	3	Melakukan pengecekan secara rutin di bagian software	4	72
R3.3		Kerusakan kapersky	Memunculkan celah keamanan pada teller	6	Tidak adanya dokumen pendukung terkait penanganan kerusakan software	4	Melakukan pengecekan secara rutin di bagian software	4	96
R3.4		Kerusakan kapersky	Memunculkan celah keamanan pada teller	6	Telat melakukan perpanjangan lisensi	4	Melakukan pengecekan secara rutin di bagian software	4	96
R3.5		Kegagalan sistem operasi	Proses bisnis terhambat pada bagian teller yaitu tidak dapat melakukan	6	Tidak adanya prosedur penginstallan sistem	4	Melakukan pengecekan secara rutin di bagian software	4	96

Code	Process Function (Step)	Potential Failure Modes (process defects)	Potential Effect(s) of Failure	SEV	Potential Cause(s) of Failure	OCC	Current Process Controls	DET	RPN
			proses input data		operasi				
R3.6		Kegagalan sistem operasi	Proses bisnis terhambat pada bagian teller yaitu tidak dapat melakukan proses input data	6	Software tidak dapat mendeteksi aplikasi tidak berlisensi	7	Adanya pendeteksi IP	4	168
R3.7		Kegagalan sistem operasi	Kerugian finansial	6	Bencana alam	3	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	72
R3.8		Kegagalan sistem operasi	Proses bisnis terhambat pada bagian teller yaitu tidak dapat melakukan proses input data	6	Telat melakukan perpanjangan lisensi	3	Melakukan pengecekan secara rutin terhadap software	4	72
R3.9		Kerusakan aplikasi sistem (F@st,Host,SVS)	Proses bisnis terganggu di bagian transaksi nasabah	5	Kesalahan melakukan prosedur penggunaan sistem	5	Melakukan pengecekan terhadap sistem transaksi	4	100
R3.10		Kerusakan aplikasi sistem (F@st,Host,SVS)	Proses bisnis terganggu di bagian transaksi nasabah	5	Software masih terdapat celah keamanan	5	Adanya software anti virus	4	100
R3.11		Kerusakan aplikasi sistem (F@st,Host,SVS)	Kerugian finansial	5	Tidak adanya prosedur penanganan	4	Melakukan pengecekan secara secara rutin terhadap keamanan sistem setiap bulan	4	80

Code	*Process Function (Step)*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
					kesalahan penggunaan aplikasi				
R3.12		Kerusakan aplikasi sistem (F@st,Host,SVS)	Kerugian finansial	5	Bencana alam	2	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	2	20

Hasil Analisis Risiko Tim B

Hasil analisis risiko yang dilakukan oleh Tim B pada teller Bank XYZ dimana tim B terdiri dari seorang yang telah menguasai metode FMEA, dan seorang narasumber yang sama dari Manager Operation Bank XYZ yang juga telah memahami konsep penggunaan FMEA.

Tabel 4.5.1.2. Hasil Analisis Risiko Tim B (Sumber: Peneliti, 2014)

Code	*Process Function (Step)*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
R1.1	Informasi	Pembobolan informasi	Penyebaran informasi perusahaan	9	Sharing password yang dilakukan oleh karyawan	3	Adanya SOP terkait sharing password karyawan	6	162
R1.2		Pembobolan informasi	Penyebaran informasi perusahaan	9	Sistem disadap oleh penyadap	4	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	4	144
R1.3		Pembobolan informasi	Kerugian finansial	9	Bencana alam	1	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	2	18
R1.4		Kegagalan sistem transaksi	Penyebaran informasi perusahaan	9	Kesalahan dalam melakukan input transaksi	7	Pengecekkan terhadap sistem transaksi setiap hari	6	378

Code	*Process Function (Step)*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
R1.5		Kegagalan sistem transaksi	Kerugian finansial	9	Bencana alam	1	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	7	63
R1.6		Kegagalan sistem transaksi	Kerugian finansial	9	Sistem mati dan tidak dapat diakses	7	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	9	567
R2.1	Hardware	Kerusakan server	Server tidak dapat digunakan	8	Kebocoran pada ruangan server	8	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	7	448
R2.2		Kerusakan server	Server tidak dapat digunakan	8	Kesalahan dalam konfigurasi	4	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	7	224
R2.3		Kerusakan server	Kerugian finansial	7	Keruntuhan bangunan	1	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	7	49
R2.4		Kerusakan server	Kerugian finansial	7	Bencana alam	1	Tata letak aset diletakkan pada posisi yang sesuai	5	35

Code	Process Function (Step)	Potential Failure Modes (process defects)	Potential Effect(s) of Failure	SEV	Potential Cause(s) of Failure	OCC	Current Process Controls	DET	RPN
							dengan standar		
R2.5		Kerusakan server	Server tidak dapat digunakan	8	Terjadinya kerusakan pada komponen yang ada di server : kabel putus	3	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan	7	168
R2.6		Kerusakan komputer	Proses bisnis terhambat pada bagian teller seperti menimbulkan antrian	4	Adanya virus yang menyerang	1	Adanya software untuk anti virus	10	40
R2.7		Kerusakan komputer	Proses bisnis terhambat pada bagian teller seperti menimbulkan antrian	4	Lisensi software yang digunakan sudah melebihi batas waktu	2	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan	7	56
R2.8		Kerusakan komputer	Kerugian finansial	8	Bencana alam	1	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	5	40
R2.9		Kerusakan komputer	Kerugian finansial	8	Kebocoran pada ruangan komputer	4	Melakukan pengecekkan secara rutin terhadap keamanan sistem setiap bula	10	320
R2.10		Kerusakan komputer	Kerugian finansial	9	Keruntuhan bangunan	8	Tata letak aset diletakkan pada posisi yang sesuai	5	360

Code	Process Function (Step)	Potential Failure Modes (process defects)	Potential Effect(s) of Failure	SEV	Potential Cause(s) of Failure	OCC	Current Process Controls	DET	RPN
							dengan standar		
R2.11		Kerusakan komputer	Proses bisnis terhambat pada bagian teller seperti menimbulkan antrian	4	Terjadinya kerusakan pada komponen yang ada pada komputer : monitor rusak,keyboard rusak dll	5	Melakukan pengecekan secara secara rutin terhadap keamanan sistem setiap bulan	7	140
R2.12		Kerusakan pada intranet, internet, hub dan router	Tidak dapat diakses secara rela time	10	Kesalahan dalam melakukan konfigurasi	6	Melakukan pengecekan secara secara rutin terhadap keamanan sistem setiap bulan	7	420
R2.13		Kerusakan pada intranet, internet, hub dan router	Proses bisnis terhambat pada bgian teller yaitu komunikasi di bagian teller tidak menjadi lancar	4	Maintenance yang tidak rutin	7	Melakukan pengecekan secara secara rutin terhadap keamanan sistem setiap bulan	6	168
R2.14		Kerusakan pada intranet, internet, hub dan router	Proses bisnis terhambat pada bgian teller yaitu komunikasi di bagian teller tidak menjadi lancar	4	Adanya hacker yang dapat masuk pada sistem melalui celah pengggunaan internet	4	Adanya pendeteksi IP yang tidak terdaftar	5	80

Code	*Process Function (Step)*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
R2.15		Kerusakan pada intranet, internet, hub dan router	Kerugian finansial	10	Bencana alam	3	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	120
R2.16		Kerusakan pada intranet, internet, hub dan router	Kerugian finansial	10	Keruntuhan bangunan	1	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	4	40
R2.17		Kerusakan pada intranet, internet, hub dan router	Teller Bank XYZ kembali menggunakan sistem konvensional	8	Terjadinya kerusakan pada hub dan router	4	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	3	96
R2.18		Kerusakan hadrware pendukung	Proses bisnis terhambat yaitu menimbulkan antrian nasabah	4	Komponen penyusun hardware pendukung tidak asli	1	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	3	12
R2.19		Kerusakan hardware pendukung	Proses bisnis terhambat pada bagian teller seperti menimbulkan antrian	4	Prosedur maintenance hardware tidak dilakukan secara rutin	7	Melakukan pengecekan secara rutin terhadap keamanan sistem setiap bulan sekali	4	112
R2.20		Kerusakan hardware	Kerugian finansial	10	Adanya bencana alam di area Bank	1	Tata letak aset diletakkan pada posisi yang sesuai	9	90

Code	Process Function (Step)	Potential Failure Modes (process defects)	Potential Effect(s) of Failure	SEV	Potential Cause(s) of Failure	OCC	Current Process Controls	DET	RPN
		pendukung			XYZ		dengan standar		
R3.1	Software	Kerusakan kapersky	Kerugian finansial	9	Bencana alam	1	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	9	81
R3.2		Kerusakan kapersky	Proses bisnis terhambat pada bagian teller yaitu sistem menjadi terkena virus	9	Software tidak dapat melakukan update secara otomatis	6	Melakukan pengecekan secara rutin di bagian software	7	378
R3.3		Kerusakan kapersky	Memunculkan celah keamanan pada teller	9	Tidak adanya dokumen pendukung terkait penanganan kerusakan software	3	Melakukan pengecekan secara rutin di bagian software	6	162
R3.4		Kerusakan kapersky	Memunculkan celah keamanan pada teller	9	Telat melakukan perpanjangan lisensi	3	Melakukan pengecekan secara rutin di bagian software	6	162
R3.5		Kegagalan sistem operasi	Proses bisnis terhambat pada bagian teller yaitu tidak dapat melakukan proses input data	9	Tidak adanya prosedur penginstallan sistem operasi	1	Melakukan pengecekan secara rutin di bagian software	6	54
R3.6		Kegagalan sistem operasi	Proses bisnis terhambat pada bagian teller yaitu	9	Software tidak dapat mendeteksi aplikasi	4	Adanya pendeteksi IP	5	180

Code	*Process Function (Step)*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
			tidak dapat melakukan proses input data		tidak berlisensi				
R3.7		Kegagalan sistem operasi	Kerugian finansial	9	Bencana alam	3	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	9	243
R3.8		Kegagalan sistem operasi	Proses bisnis terhambat pada bagian teller yaitu tidak dapat melakukan proses input data	9	Telat melakukan perpanjangan lisensi	1	Melakukan pengecekan secara rutin terhadap software	6	54
R3.9		Kerusakan aplikasi sistem (F@st,Host,SVS)	Proses bisnis terganggu di bagian transaksi nasabah	9	Kesalahan melakukan prosedur penggunaan sistem	1	Melakukan pengecekan terhadap sistem transaksi	6	54
R3.10		Kerusakan aplikasi sistem (F@st,Host,SVS)	Proses bisnis terganggu di bagian transaksi nasabah	9	Software masih terdapat celah keamanan	2	Adanya software anti virus	7	126
R3.11		Kerusakan aplikasi sistem (F@st,Host,SVS)	Kerugian finansial	9	Tidak adanya prosedur penanganan kesalahan penggunaan aplikasi	1	Melakukan pengecekan secara secara rutin terhadap keamanan sistem setiap bulan	6	54

Code	*Process Function (Step)*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
R3.12		Kerusakan aplikasi sistem (F@st,Host,SVS)	Kerugian finansial	9	Bencana alam	3	Tata letak aset diletakkan pada posisi yang sesuai dengan standar	9	243

4.5.2. Rangking RPN

Setelah ditentukan nilai *severity*, *occurrence* dan *detection* maka didapatkan nilai RPN untuk masing-masing risiko yang ada. Berikut ini merupakan urutan risiko berdasarkan nilai RPN.

Tabel 4.5.2.1. Pengkategorian RPN (Sumber: FMEA)

Level Risiko	Skala Nilai RPN
Very low	x < 20
Low	20≤ x <80
Medium	80≤ x <120
High	120≤ x <200
Very high	x>200

Dengan adanya pengkategorian RPN, maka dapat diketahui risiko yang memiliki nilai RPN tertinggi hingga terendah berdasarkan pengkategorian RPN. Maka hasil analisis risiko yang telah dilakukan oleh tim A dan tim B, dilakukan pengurutan RPN tertinggi hingga terendah, yaitu:

Rangking RPN Tim A

Hasil rangking RPN yang telah dilakukan oleh tim A, dimana tim A membuat batasan pada ketegori risiko sangat tinggi dan tinggi hanya diberi batasan satu risiko.

Tabel 4.5.2.2. Tabel Pengkategorian RPN (Sumber: Peneliti, 2014)

Kode	Risiko	Penyebab	*RPN*	Kategori
R2.2	Kerusakan server	Kesalahan dalam konfigurasi	240	**Very High**
R3.6	Kegagalan sistem operasi	Software tidak dapat mendeteksi aplikasi tidak berlisensi	168	**High**
R2.20	Kerusakan hardware pendukung	Adanya bencana alam di area Bank XYZ	120	**Medium**

Kode	Risiko	Penyebab	*RPN*	Kategori
R2.7	Kerusakan komputer	Lisensi software yang digunakan sudah melebihi batas waktu	120	**Medium**
R2.8	Kerusakan komputer	Bencana alam	120	**Medium**
R2.6	Kerusakan komputer	Adanya virus yang menyerang	112	**Medium**
R2.3	Kerusakan server	Keruntuhan bangunan	112	**Medium**
R3.9	Kerusakan aplikasi sistem (F@st,Host,SVS)	Kesalahan melakukan prosedur penggunaan sistem	100	**Medium**
R3.10	Kerusakan aplikasi sistem (F@st,Host,SVS)	Software masih terdapat celah keamanan	100	**Medium**
R3.3	Kerusakan kapersky	Tidak adanya dokumen pendukung terkait penanganan kerusakan software	96	**Medium**
R3.4	Kerusakan kapersky	Telat melakukan perpanjangan lisensi	96	**Medium**
R3.5	Kegagalan sistem operasi	Tidak adanya prosedur penginstallan sistem operasi	96	**Medium**
R2.4	Kerusakan server	Bencana alam	96	**Medium**
R2.1	Kerusakan server	Kebocoran pada ruangan server	80	**Medium**
R2.17	Kerusakan pada intranet, internet, hub dan router	Terjadinya kerusakan pada hub dan router	80	**Medium**
R3.11	Kerusakan aplikasi sistem (F@st,Host,SVS)	Tidak adanya prosedur penanganan kesalahan penggunaan aplikasi	80	**Medium**
R1.5	Kegagalan sistem transaksi	Bencana alam	72	**Low**
R2.15	Kerusakan pada intranet, internet, hub dan router	Bencana alam	72	**Low**
R3.2	Kerusakan kapersky	Software tidak dapat melakukan update secara otomatis	72	**Low**
R3.7	Kegagalan sistem operasi	Bencana alam	72	**Low**
R3.8	Kegagalan sistem	Telat melakukan perpanjangan	72	**Low**

Kode	Risiko	Penyebab	*RPN*	Kategori
	operasi	lisensi		
R2.9	Kerusakan komputer	Kebocoran pada ruangan komputer	72	**Low**
R2.18	Kerusakan hadrware pendukung	Komponen penyusun hardware pendukung tidak asli	60	**Low**
R2.19	Kerusakan hardware pendukung	Prosedur maintenance hardware pendukung dilakukan setiap bulan	60	**Low**
R1.3	Pembobolan informasi	Bencana alam	56	**Low**
R2.10	Kerusakan komputer	Keruntuhan bangunan	50	**Low**
R2.5	Kerusakan server	Terjadinya kerusakan pada komponen yang ada di server : kabel putus	48	**Low**
R1.6	Kegagalan sistem transaksi	Sistem mati dan tidak dapat diakses	48	**Low**
R2.16	Kerusakan pada intranet, internet, hub dan router	Keruntuhan bangunan	48	**Low**
R3.1	Kerusakan kapersky	Bencana alam	48	**Low**
R2.11	Kerusakan komputer	Terjadinya kerusakan pada komponen yang ada pada komputer : monitor rusak,keyboard rusak dll	40	**Low**
R2.12	Kerusakan pada intranet, internet, hub dan router	Kesalahan dalam melakukan konfigurasi	40	**Low**
R2.13	Kerusakan pada intranet, internet, hub dan router	Maintenance yang tidak rutin	40	**Low**
R1.4	Kegagalan sistem transaksi	Kesalahan dalam melakukan input transaksi	36	**Low**
R2.14	Kerusakan pada intranet, internet, hub dan router	Adanya hacker yang dapat masuk pada sistem melalui celah pengggunaan internet	36	**Low**
R1.1	Pembobolan informasi	Sharing password yang dilakukan oleh karyawan	28	**Low**
R1.2	Pembobolan	Sistem disadap oleh penyadap	28	**Low**

Kode	Risiko	Penyebab	RPN	Kategori
	informasi			
R3.12	Kerusakan aplikasi sistem (F@st,Host,SVS)	Bencana alam	20	Low

Rangking RPN Tim B

Hasil rangking RPN yang telah dilakukan oleh tim B, penilaian risiko yang dihasilkan oleh tim B menghasilkan 10 risiko yang memiliki kategori risiko tertinggi dan 10 risiko dengan ketegori risiko tingg. Hasil RPN yang didapatkan tidak diberikan batasan hanya satu risiko saja untuk kategori very high dan high. Tetapi, hasil RPN yang dihasilkan berdasarkan penilaian yang dilakukan dengan melihat dokumen mengenai hasil audit yang dilakukan pada penggunaan teknologi informasi pada teller Bank XYZ sebagai acuan dalam melakukan penilaian risiko.

Tabel 4.5.2.3. Ranking RPN Tim B (Sumber: Peneliti, 2014)

Kode	Risiko	Penyebab	RPN	Kategori
R1.6	Kegagalan sistem transaksi	Sistem mati dan tidak dapat diakses	567	Very High
R1.7	Kerusakan server	Kebocoran pada ruang server	448	Very High
R2.12	Kerusakan pada intrenet, internet, hub dan router	Kesalahan dalam melakukan konfigurasi	420	Very High
R1.4	Kegagalan sistem transaksi	Kesalahan dalam melakukan input transaksi	378	Very High
R3.2	Kerusakan kapersky	Software tidak dapat melakukan update otomatis	378	Very High
R2.10	Kerusakan komputer	Kerugian financial	360	Very High

Kode	Risiko	Penyebab	*RPN*	Kategori
R2.9	Kerusakan komputer	Kebocoran pada ruangan komputer	320	**Very High**
R3.7	Kegagalan sistem operasi	Telat melakukan perpangjangan lisensi	243	**Very High**
R3.12	Kerusakan aplikasi sistem (F@st,Host,SVS)	Bencana alam	243	**Very High**
R2.2	Kerusakan server	Kesalahan dalam melakukan konfigurasi	224	**Very High**
R3.6	Kegagalan sistem operasi	Software tidak dapat mendeteksi aplikasi tidak berlisensi	180	**High**
R2.5	Kerusakan server	Server tidak dapat diguanakan	168	**High**
R2.13	Kerusakan pada intranet, internet, hub dan router	Maintenance yang tidak rutin	168	**High**
R1.1	Pembobolan informasi	Sharing password yang dilakukan oleh karyawan	162	**High**
R3.3	Kerusakan kapersky	Tidak adanya dokumen pendukung terkait penanganan kerusakan software	162	**High**
R3.4	Kegagalan sistem operasi	Tidak adanya prosedur penginstalan sistem operasi	162	**High**
R1.2	Pembobolan informasi	Sistem disadap oleh penyadap	144	**High**
R2.11	Kerusakan komputer	Terjadinya kerusakan pada komponen yang ada pada komputer: monitor rusak, keyboard rusak,dll	140	**High**
R2.15	Kerusakan pada intranet, internet, hub dan router	Bencana alam	120	**High**
R3.10	Kerusakan aplikasi sistem (F@st,Host,SVS)	Software masih terdapat celah keamanan	126	**High**
R2.19	Kerusakan hardware pendukung	Prosedur maintenence hardware tidak dilakukan secara rutin	112	**Medium**
R2.17	Kerusakan pada	Terjadinya kerusakan pada hub	96	**Medium**

Kode	Risiko	Penyebab	*RPN*	Kategori
	internet, intranet, hub dan router	dan router		
R2.20	Kerusakan hardware pendukung	Adanya bencana alam di area Bank XYZ	90	**Medium**
R3.1	Kerusakan kapersky	Bencana alam	81	**Medium**
R2.14	Kerusakan pada internet, intranet, hub dan router	Adanya hacker yang dapat masuk pada sistem melalui celah pengggunaan internet	80	**Medium**
R1.5	Kegagalan sistem transaksi	Bencana alam	63	**Low**
R2.7	Kerusakan komputer	Lisensi software yang digunakan sudah melebihi batas waktu	56	**Low**
R3.5	Kegagalan sistem operasi	Tidak adanya prosedur penginstallan sistem operasi	54	**Low**
R3.8	Kegagalan sistem operasi	Telat melakukan perpanjangan lisensi	54	**Low**
R3.9	Kerusakan aplikasi sistem (F@st,Host,SVS)	Kesalahan melakukan prosedur penggunaan sistem	54	**Low**
R3.11	Kerusakan aplikasi sistem (F@st,Host,SVS)	Tidak adanya prosedur penanganan kesalahan penggunaan aplikasi	54	**Low**
R2.3	Kerusakan server	Keruntuhan bangunan	49	**Low**
R2.6	Kerusakan komputer	Adanya virus yang menyerang	40	**Low**
R2.8	Kerusakan komputer	Bencana alam	40	**Low**
R2.16	Kerusakan pada intranet, internet, hub dan router	Keruntuhan bangunan	40	**Low**
R2.4	Kerusakan server	Bencana alam	35	**Low**
R2.18	Pembobolan informasi	Bencana alam	18	**Very Low**
R1.3	Kerusakan hadrware pendukung	Komponen penyusun hardware pendukung tidak asli	12	**Very Low**

4.6. Analisis Kesenjangan

Analisis kesenjangan bertujuan untuk mengetahui kesenjangan dari penilaian risiko yang dilakukan oleh dua tim yang berbeda, yaitu tim A dan tim B dalam melakukan penilaian risiko menggunakan metode FMEA. Sehingga, hasil penilaian yang telah dilakukan kemudian dilakukan analisis kesenjangan untuk mengetahui faktor yang mempengaruhi perbedaan hasil dari pemrioritasan risiko pada RPN yang dihasilkan berdasarkan kondisi tim A dan tim B ketika melakukan penilaian. Sehingga dari penggunaan metode Analisis Kesenjangan, didapatkan usulan yang dapat dijadikan referensi untuk membuat formulasi Kerangka FMEA yang Disesuaikan.

Tabel 4.6.1. Hasil Analisis Kesenjangan pada Penilaian Risiko yang Dilakukan oleh Tim A dan Tim B (Sumber: Peneliti, 2014)

Analisis Kesenjangan			
Kategori	**Kondisi Tim A**	**Kondisi Tim B**	**Usulan**
Prosedur	Tim A belum menggunakan prosedur untuk menjadi acuan dalam menuntun narasumber melakukan pemberian nilai risiko yang hanya berdasarkan pada acuan definisi pemberian nilai FMEA untuk menilai *severity*, *occurency*, dan *detection*.	Tim B juga telah menggunakan prosedur untuk menjadi acuan dalam menuntun narasumber melakukan pemberian nilai risiko dengan menggunakan hasil dokumen audit yang telah dilakukan pada teller bank XYZ.	Adanya prosedur penilaian risiko menggunakan metode FMEA sebagai panduan yang menjelaskan langkah-langkah penilaian risiko sehingga penilaian risiko menjadi konsisten.

Metode Pemrioritasan	Skala yang digunakan untuk memberikan nilai pada setiap kategori *severity, occurence*, dan *detection* menggunakan skala 1-10.	Skala yang digunakan untuk memberikan nilai pada setiap kategori *severity, occurence,* dan *detection* menggunakan skala 1-10.	Skala penilaian pada setiap kategori pada *severity, occurence,* dan *detection* harus diseragamkan untuk menghasilkan pemrioritasan risiko yang sama.
Pengetahuan Narasumber	Narasumber pada penelitian adalah Manager Operation Bank XYZ, yang belum mengetahui bagaimana penggunaan metode FMEA secara detail hanya mendapatkan penjelasan secara garis besar dari fasilitator. Narasumber tidak terlibat langsung dalam melakukan penilaian risiko, hanya memberikan informasi berdasarkan pertanyaan yang ajukan oleh tim fasilitator	Narasumber pada penelitian yang dilakukan oleh tim B adalah Manager Operation Bank XYZ yang sama dengan tim A. Manager Operation telah memahami penggunaan metode FMEA secara detail bagaimana memberikan penilaian pada setiap kategori pada FMEA, yaitu *severity, occurence*, dan *detection*. Penilaian pada tiap kategori dilakukan berdasarkan panduan penilaian yang telah disediakan oleh FMEA, berdasarkan skala yang telah ditentukan dengan skala 1-10	Narasumber sebagai pihak yang berwenang dalam melakukan penilaian risiko harus mengusai *tools* yang digunakan.

		untuk memberikan nilai pada setiap kategori.	
Kemampuan Fasilitator	Fasilitator FMEA pada tim A adalah dua orang mahasiswa yang telah mengambil mata kuliah Manajemen Risiko Teknologi Informasi dan telah mempelajari penerapan FMEA dalam melakukan penilaian risiko. Penilaian risiko pada penggunaan teknologi informasi pada teller Bank XYZ dilakukan berdasarkan hasil wawancara yang telah dilakukan dengan narasumber.	Fasilitator FMEA pada tim B adalah seorang mahasiswa yang telah mengambil mata kuliah Manajemen Risiko dan telah mempelajari dan menerapkan beberapa studi kasus pada perusahaan lain terkait penggunaan metode FMEA dalam melakukan penilaian risiko. Fasilitotr FMEA pada tim B ini berperan dalam memandu narasumber, Manajer Operation dalam melakukan penilaian risiko yang dilakukan dengan menggunakan panduan FMEA dan referensi dokumen audit untuk melakukan penilaian, hal ini dilakukan untuk menghindari pemberian nilai yang subjektif.	Fasilitator FMEA dapat memberikan panduan yang tepat dalam melakukan penilaian risiko menggunakan FMEA sesuai dengan panduan dari FMEA yang disesuaikan dengan prosedur dan kebijakan yang telah diterapkan oleh Perusahaan terkait dengan kegiatan manajemen risiko teknologi informasi.

4.7. Metode Kualitatif

Hasil penilaian risiko menggunakan metode FMEA yang telah dilakukan dan berdasarkan hasil analisis kesnjangan, kemudian dilakukan pengujian dengan metode kualitatif untuk mendukung konsistensi hasil penilaian risiko menggunakan metode FMEA

4.7.1. Hasil Wawancara Penilaian Risiko Penerapan Teknologi Informasi pada Teller Bank XYZ

Berdasarkan hasil wawancara yang telah dilakukan dalam melakukan penilaian risiko pada penggunaan teknologi informasi pada teller Bank XYZ. Hasil penilian risiko terkait penggunaan teknologi informasi didapatkan hasil tingkat keparahan, frekuensi kejadian, dan cara deteksi yang dilakukan terhadap menangani risiko tersebut. Dan dibutuhkan biaya untuk mempersiapkan penanganan pada risiko yang mungkin terjadi untuk melakukan pencegahan dan merencanakan cara mitigasi terhadap ancaman yang terjadi. Sehingga, dalam melakukan penilian risiko harus dipastikan kekonsistenan dari risiko tertinggi yang mungkin terjadi pada penggunaan teknologi informasi pada teller Bank XYZ.

Berikut kutipan dari hasil wawancara dengan Manager Operasional Bank XYZ "**MO**":

> "Perusahaan kami dalam melakukan penilaian risiko, ada beberapa hal yang harus dipersiapkan, seperti menyiapkan dokumen panduan dan prosedur. Agar proses penilaian risiko sesuai dengan kebijakan yang telah ditetapkan oleh perusahaan dan sesuai dengan kebijakan Bank Indonesia dalam melakukan manajemen risiko." **Wcr.inf01.MO.stat01**

> "Dalam sistem yang kami gunakan untuk melakukan pemrioritasan risiko dilakukan secara otomatis oleh sistem, karena sistem telah diatur dengan ketentuan dan batasan-batasan yang telah disepakati oleh perusahaan. Karena jika metode yang digunakan berbeda-

beda dapat mempengaruhi pemrioritasan risiko tertinggi. Jadi, dengan adanya kesepakatan metode yang sama, walaupun penilian risiko dilakukan oleh tim yang berbeda tidak akan menjadi masalah besar." **Wcr.inf01.MO.stat02**

"Penilaian risiko dilakukan oleh orang-orang yang berkompeten dibidangnya dan memiliki tugas atau wewenang dalam melakukan penilaian risiko yang telah mendapatkan pelatihan." **Wcr.inf01. MO.stat03**

"Jika adanya metode baru dalam melakukan penilaian risiko, seorang fasilitator harus memiliki pengetahuan dan kemampuan yang baik dalam menjelaskan metode yang digunakan dalam melakukan penilian risiko. Sehingga tidak ada kesalahpahaman dalam menerima informasi yang disampaikan oleh faslilitator pada pihak kami, jika ingin melakukan penelitian di perusahaan." **Wcr.inf01.MO.stat04**

4.7.2. Profil Informan

Profil informan yang sesuai untuk melakukan penilaian risiko, J. Allen berpendapat orang yang melakukan manajemen risiko pada perusahaan ialah orang yang memiliki keterampilan dalam melakukan managemen risiko dan menawarkan visi positif untuk mencapai keberhasilan (J. Allen, 2008). Orang yang sesuai dalam melakukan analisis risiko adalah orang yang mampu memiliki strategi-strategi untuk menghasilkan cara-cara baru atau langkah-langkah baru yang kreatif untuk masa depan, mampu mengidentifikasi apa yang menjadi hal penting dan mencari solusi, serta mampu menyiapkan layanan yang mampu dan siap menghadapi tantangan yang ada (DOH, 2007).

Bates dan Sillberman menyampaikan tujuh kriteria positif dalam melakukan penilaian risiko, yaitu (Silberman, 2008):

- ***Involvement of Service Users and Relatives in Risk Assessment***

  Melibatkan orang yang bersangkutan dalam melalukan pengumpulan informasi terkait penggunaan aset kritis yang akan dilakukan penilian risiko. Sehingga mampu menghasilkan ide-ide dan solusi ketika melakukan evaluasi, dan mengamati sejauh mana karyawan mampu paham mengenai perang dan tanggung jawab untuk terhadap penggunaan aset kritis dan mampu mengambil keputusan-keputasan yang bijak yang ada keterkaitannya dengan risiko.

- ***Positive and Informed Risk Taking***

  Proses ini dilakukan berdasarkan sudut pandang positif yang dilakukan oleh penilai risiko terhadap orang, dalam penelitian ini berkaitan dengan karyawan. Bagaimana dapat melihat kemampuan yang dimiliki orang tiap karyawan dan memberikan apresiasi untuk menjaga keberadaan karyawan sehingga merasa tetap nyaman dan aman ketika mengambil risiko.

- ***Proportionality***

  Manajemen risiko harus sesuai dengan potensi bahaya dimana semakin serius masalah yang mungkin terjadi makan semakin banyak orang, waktu, dan biaya yang dibutuhkan.

- ***Contextualising Behaviour***

  Kaitannya dengan perilaku, adalah proses untuk melakukan pengumpulan informasi berdasarkan sejarah pengalaman dari masalah risiko yang pernah terjadi dan bagaimana pandangan orang, dalam hal ini karyawan dalam memandang masalah risiko yang pernah terjadi. Sehingga sumber-sumber pendapat dan catatan historis mampu menghasilkan respon-repon terbaik. Cara penyampaian pertanyaan dapat menggunakan (4+1), *What have we tried? what have we learned? What are we pleased about? what are we concerned about?*

  Sehingga dari pertanyaan menggunakaan (4+1) mampu menghasilkan pemahaman mengenai perilaku seseorang dalam konteks yang berbeda.

- ***Defensible Decision Making***

  Adanya alasan yang jelas untuk mengambil keputusan dalam melakukan manajemen risiko, bagaimana melakukan tindakan terhadap risiko yang ada berdasarkan kebijakan ataupun undang-undang atau peraturan yang telah mengatur pengambilan keputusan dalam melakukan manajemen risiko.

- ***A Learning Culture***

  Cara yang dilakukan untuk membangun budaya belajar pada perusahaan agar tidak mengulang kesalahan yang sama pada risiko yang pernah terjadi dapat menerapkan pertanyaan

menggunakan 4+1 dan Apa yang bekerja atau Apa yang tidak bekerja. Sehingga mampu membuat kontribusi yang signifikan untuk membangun budaya belajar dalam perusahaan.

- ***Tolerable Risks***
  Proses ini berkaitan dengan bagaimana seseorang mampu mengambil pendekatan yang lebih seimbang yang berkaitan dengan risiko yang mungkin terjadi terhadap setiap tindakan yang dilakukan. Sehingga seseorang mampu mempertimbangkan cara yang masuk akal agar tetap menjaga kemungkinan yang terjadi dalam keadaan yang tetap aman.

Cara yang dilakukan untuk menentukan profil informan dalam kaitannya untuk melakukan manajemen risiko pada teller Bank XYZ berdasarkan kriteria di atas, maka profil informan yang memiliki tanggung jawab mengetahui kondisi lapangan, dan mampu melakukan penilaian risiko pada perusahaan ini, adalah *Manager Operation* perusahaan Bank XYZ. *Manager Operation*, bertanggung jawab atas kegiatan operasi yang ada pada kantor cabang terkait dengan risiko yang mungkin terjadi pada kegiatan operasional perusahaan.

4.7.3. Metode Pemprioritasan Berpengaruh pada Konsistensi Penggunaan Metode FMEA dalam Melakukan Pemrioritasan Risiko

Metode yang digunakan dalam melakukan pemrioritasan nilai risiko yang ada pada teller Bank XYZ berpengaruh pada konsistensi penggunaan metode FMEA jika dilakukan penilaian oleh dua atau lebih tim yang melakukan penilaian risiko. Prosedur pada penggunaan metode dalam melakukan penilaian risiko memiliki batasan yang diambil untuk membuat kesepakatan dalam melakukan analisis, membuat rekomendasi perbaikan, pelaksanaan perbaikan, dll dalam melakukan penilaian risiko menggunakan metode FMEA (Failure Modes and Effects Analysis Guide, 2008). Sehingga untuk mendukung pernyataan ini dilakukan wawancara terhadap narasumber.

Dari hasil wawancara yang telah dilakukan, maka didapatkan hasil mengenai metode pemprioritasan risiko pada teller Bank XYZ yang disebabkan oleh oleh hal-hal berikut :

1. Tim A dan tim B sudah menggunakan skala pemberian nilai risiko yang sama untuk nilai *severity, occurency*, dan *detection* dengan skala 1-10 dimana dengan nilai 10 pada *severity* menunjukkan tingkat keparahan yang tinggi pada risiko yang terjadi berpengaruh pada keberlangsungan proses bisnis dan nilai <10 tingkat keparahan yang timbulkan semakin kecil. Pada penilaian *occurency*, nilai 10 diberikan pada risiko yang kemungkinan terjadi lebih dari 1 kali dalam seharinya dan nilai <10 frekuensi terjadi risiko semakin rendah. Sedangkan pada detection, pemberian nilai 10 pada risiko yang tingkat deteksinya sulit untuk dicegah dan nilai <10 risiko yang terjadi

semakin mudah untuk dideteksi. Pembahasan petunjuk penilaian risiko menggunakan FMEA dapat dilihat pada Tabel 2.3.1 – 2.3.3. "Dalam sistem yang kami gunakan untuk melakukan pemrioritasan risiko dilakukan secara otomatis oleh sistem, karena sistem telah diatur dengan ketentuan dan batasan-batasan yang telah disepakati oleh perusahaan. Karena jika metode yang digunakan berbeda-beda dapat mempengaruhi pemrioritasan risiko tertinggi. Jadi, dengan adanya kesepakatan metode yang sama, walaupun penilian risiko dilakukan oleh tim yang berbeda tidak akan menjadi masalah besar." **Wcr.inf01.MO.stat02**

Pentingnya penyamaan dalam pemberian nilai pada skala dalam rangka mendukung prioritas risiko dengan menggunakan skala penilaian dari FMEA. Skala penilaian pada FMEA memiliki beberapa ragam, seperti skala 1-5, 1-10, 1-20, dsb. Skala ini bisa diubah dan disesuaikan dengan kondisi dan kebutuhan perusahaan berdasarkan hasil evaluasi dan kesepakatan yang ditetapkan oleh perusahaan (Failure Modes and Effects Analysis Guide, 2008).

4.7.4. Prosedur Penilaian Berpengaruh pada Konsistensi Penggunaan Metode FMEA dalam Melakukan Pemrioritasan Risiko

Prosedur yang digunakan dalam melakukan pemrioritasan nilai risiko yang ada pada teller Bank XYZ berpengaruh pada konsistensi penggunaan metode FMEA jika dilakukan penilaian oleh dua atau lebih tim yang melakukan penilaian risiko. Hal ini juga disampaikan oleh Robillard mengenai adanya panduan untuk membimbing penggunaan pendekatan yang digunakan oleh perusahaan secara sistematis dalam melakukan manajemen risiko (Integrated Risk Management Framework, 2011). Sehingga

untuk mendukung pernyataan ini dilakukan wawancara terhadap narasumber.

Dari hasil wawancara yang telah dilakukan, maka didapatkan hasil :

Adanya penggunaan prosedur yang telah menjadi kesepakatan tim fasilitator FMEA dan perusahaan dalam melakukan penilaian risiko. Penggunaan prosedur dapat menjadi panduan dalam melakukan penilaian risiko apa saja yang perlu disiapkan dan bagaimana alur penilaian yang digunakan. Sehingga, dengan adanya prosedur yang telah mengatur untuk melakukan penilaian risiko tidak terjadi permasalahan yang besar jika dilakukan oleh tim yang berbeda. "Perusahaan kami dalam melakukan penilaian risiko, ada beberapa hal yang harus dipersiapkan, seperti menyiapkan dokumen panduan dan prosedur. Agar proses penilaian risiko sesuai dengan kebijakan yang telah ditetapkan oleh perusahaan dan sesuai dengan kebijakan Bank Indonesia dalam melakukan menajemen risiko." **Wcr.inf01. MO.stat01**

4.7.5. Pengetahuan Narasumber Berpengaruh pada Konsistensi Penggunaan Metode FMEA dalam Melakukan Pemrioritasan Risiko

Pengetahuan narasumber berpengaruh pada pemrioritasan nilai risiko yang ada pada teller Bank XYZ menggunakan metode dalam melakukan penilaian risiko. Pengetahuan narasumber terhadap analisis penialaian risiko menggunakan metode FMEA juga berpengaruh pada performa tim FMEA dalam melakukan penilaian, apakah telah melakukan penilaian pada narasumber yang benar dan bertanggung jawab atas aset kritis yang dilakukan analisis risiko (Villacourt, 1992). Sehingga untuk mendukung pernyataan ini dilakukan wawancara terhadap narasumber.

Dari hasil wawancara yang telah dilakukan, maka didapatkan hasil :

Narasumber yang dijadikan sumber informasi dalam penelitian memiliki pengtahuan dan informasi

mengenai kegiatan operasional dari proses bisnis yang ingin dilakukan analisis risiko, dalam penelitian ini, penggunaan teknologi informasi pada teller Bank. Dan narasumber telah memiliki pengetahuan atau tanggung jawab dalam melakukan penilaian risiko. Sehingga memudahkan penelitian untuk melakukan analisis risiko dan perhitungan risiko menggunakan metode FMEA. "Penilaian risiko dilakukan oleh orang-orang yang berkompeten dibidangnya dan memiliki tugas atau wewenang dalam melakukan penilaian risiko yang telah mendapatkan pelatihan." **Wcr.inf01.MO.stat03**

4.7.6. Kemampuan Fasilitator FMEA Berpengaruh pada Konsistensi Penggunaan Metode FMEA dalam Melakukan Pemrioritasan Risiko

Kemampuan fasilitator FMEA berpengaruh pada pemrioritasan nilai risiko yang ada pada teller Bank XYZ menggunakan metode dalam melakukan penilaian risiko. Konsistensi antara hasil FMEA dapat ditingkatkan dengan mengembangkan keterampilan sejumlah kecil fasilitator berpengalaman yang dapat membantu para analis untuk menggunakan FMEA lebih efektif dan konsisten dengan membantu dalam definisi mode kegagalan dan peringkat keparahan, probabilitas dan indeks pendeteksian (M.T. Oldenhofa J. v.-R., 2011). Sehingga untuk mendukung pernyataan ini dilakukan wawancara terhadap narasumber.
Dari hasil wawancara yang telah dilakukan, maka didapatkan hasil :

Kemampuan fasilitator dalam melakukan penelitian analisis risiko dan penilaian risiko menggunakan metode FMEA, memiliki peran penting untuk menyampaikan bagaiamana cara mengisi penilaian risiko untuk memandu narasumber dalam memberikan penilaian. Sehingga pemrioritasan risiko yang dihasilkan sesuai dengan kondisi yang ada pada perusahaan dan sesuai dengan ketentuan dari metode FMEA yang digunakan. "Jika adanya metode baru dalam

melakukan penilaian risiko, seorang fasilitator harus memiliki pengetahuan dan kemampuan yang baik dalam menjelaskan metode yang digunakan dalam melakukan penilian risiko. Sehingga tidak ada kesalahpahaman dalam menerima informasi yang disampaikan oleh faslilitator pada pihak kami, jika ingin melakukan penelitian di perusahaan." **Wcr.inf01.MO.stat04**

4.7.7. Proposisi yang Ditemukan

Hasil penelitian yang dihasilkan menggunakan metode kualitatif yang dilakukan dengan wawancara menghasilkan pemaparan dengan proposisi minor dan proposi mayor penelitian :

4.7.7.1. Proposisi Minor

Proposisi minor dilakukan analisis dari hasil wawancara dan observasi yang telah dilakukan, sehingga ditemukan proposisi minor berdasarkan keterkaitan masing- masing domain penelitian:

1). Metode Pemrioritasan Berpengaruh pada Konsistensi Penggunaan Metode FMEA dalam Melakukan Pemrioritasan Risiko

Berdasarkan hasil wawancara yang telah dilakukan, maka didapatkan hasil bahwa Metode pemrioritasan yang digunakan dalam melakukan pemrioritasan risiko berpengaruh pada hasil konsistensi penggunaan FMEA dalam melakukan pemrioritasan risiko. Prosedur pada penggunaan metode dalam melakukan penilaian risiko memiliki batasan yang diambil untuk membuat kesepakatan dalam melakukan analisis, membuat rekomendasi perbaikan, pelaksanaan perbaikan, dll dalam melakukan penilaian risiko menggunakan metode FMEA (Failure Modes and Effects Analysis Guide, 2008).

"Metode pemrioritasan risiko berpengaruh pada hasil penilaian risiko. Tidak hanya metode saja yang dapat mempengaruhi konsistensi dalam melakukan penilaian risiko, tetapi adanya batasan atau tidak yang digunakan dalam melakukan risiko. Sehingga, dalam melakukan penilaian risiko walaupun dilakukan

oleh tim yang berbeda, metode yang digunakan harus sama." **Wcr.inf01.MO.stat02**

Hasil wawancara pada narasumber menyatakan bahwa dalam melakukan penilian risiko untuk menghasilkan konsistensi pemrioritasan risiko menggunakan metode FMEA. Cara yang dilakukan dengan membuat suatu metode yang sama dalam menentukan skala penilaian risiko dalam melakukan pembobotan penilaian. Dan ketika memberikan batasan jumlah risiko tertinggi yang ditolerir oleh perusahaan dalam hasil tingkat urgensi risiko pada level *very high risk* dan *high risk*.

2). Prosedur Penilaian Berpengaruh pada Konsistensi Penggunaan Metode FMEA dalam Melakukan Pemrioritasan Risiko

Berdasarkan hasil wawancara yang telah dilakukan, maka didapatkan hasil bahwa penggunaan prosedur dalam melakukan penilaian risiko untuk menghasilkan pemrioritasan risiko menggunakan metode FMEA, memberikan pengaruh pada hasil konsistensi penggunaan FMEA dalam melakukan pemrioritasan risiko. Hal ini juga disampaikan oleh Robillard mengenai adanya panduan untuk membimbing penggunaan pendekatan yang digunakan oleh perusahaan secara sistematis dalam melakukan manajemen risiko (Integrated Risk Management Framework, 2011).

"Perusahaan kami dalam melakukan penilaian risiko, ada beberapa hal yang harus dipersiapkan, seperti menyiapkan dokumen panduan dan prosedur. Agar proses penilaian risiko sesuai dengan kebijakan yang telah ditetapkan oleh perusahaan dan sesuai dengan kebijakan Bank Indonesia dalam melakukan manajemen risiko." **Wcr.inf01.MO.stat01**

Hasil wawancara pada narasumber menyatakan bahwa dalam melakukan penilian risiko untuk menghasilkan konsistensi pemrioritasan risiko

menggunakan metode FMEA. Cara yang dilakukan dengan membuat suatu prosedur sebagai panduan dalam melakukan penilaian risiko, sehingga dengan adanya prosedur dalam melakukan penilaian risiko. Narasumber dalam melakukan pemberian nilai risiko tidak dilakukan secara subjektif, tetapi berdarkan hasil evaluasi dan audit yang telah dilakukan oleh perusahaan dalam melakukan pemberian nilai risiko pada aset kritis perusahaan. Sehingga penilaian risiko menjadi lebih valid dibandingkan jika tidak menggunakan prosedur yang telah ditetapkan oleh perusahaan.

3). Pengetahuan Narasumber Berpengaruh pada Konsistensi Penggunaan Metode FMEA dalam Melakukan Pemrioritasan Risiko

Berdasarkan hasil wawancara yang telah dilakukan, maka didapatkan hasil bahwa pengetahuan narasumber dalam melakukan penilaian risiko untuk menghasilkan pemrioritasan risiko menggunakan metode FMEA, memberikan pengaruh pada hasil konsistensi penggunaan FMEA dalam melakukan pemrioritasan risiko. Pengetahuan narasumber terhadap analisis penialaian risiko menggunakan metode FMEA juga berpengaruh pada performa tim FMEA dalam melakukan penilaian, apakah telah melakukan penilaian pada narasumber yang benar dan bertanggung jawab atas aset kritis yang dilakukan analisis risiko (Villacourt, 1992).

> "Penilaian risiko dilakukan oleh orang-orang yang berkompeten dibidangnya dan memiliki tugas atau wewenang dalam melakukan penilaian risiko yang telah mendapatkan pelatihan. " **Wcr.inf01.MO.stat03**

Hasil wawancara pada narasumber menyatakan bahwa dalam melakukan penilian risiko untuk menghasilkan konsistensi pemrioritasan risiko menggunakan metode FMEA. Pengetahuan narasumber

memberikan pengaruh dalam melakukan penilaian risiko, sehingga dalam melakukan penilaian risiko, dapat dipastikan juga apakah narasumber telah paham bagaimana menentukan penilaian risiko pada nilai *severity*, *occurence*, dan *detection* pada tiap risiko. Sehingga penilaian risiko yang dihasilkan dapat sesuai dengan ketentuan yang telah dijelaskan pada metode FMEA dalam melakukan penilaian risiko. Dan mengurangi tingkat ketidakkonsistensian penilaian risiko jika dilakukan oleh dua tim berbeda.

4). Kemampuan Fasilitator FMEA Berpengaruh pada Konsistensi Penggunaan Metode FMEA dalam Melakukan Pemrioritasan Risiko

Berdasarkan hasil wawancara yang telah dilakukan, maka didapatkan hasil bahwa kemampuan fasilitator FMEA dalam memberikan informasi mengenai penilaian risiko yang dilakukan metode FMEA, memberikan pengaruh pada hasil konsistensi penggunaan FMEA dalam melakukan pemrioritasan risiko. Konsistensi antara hasil FMEA dapat ditingkatkan dengan mengembangkan keterampilan sejumlah kecil fasilitator berpengalaman yang dapat membantu para analis untuk menggunakan FMEA lebih efektif dan konsisten dengan membantu dalam definisi mode kegagalan dan peringkat keparahan, probabilitas dan indeks pendeteksian (M.T. Oldenhofa J. v.-R., 2011).

> "Jika adanya metode baru dalam melakukan penilaian risiko, seorang fasilitator harus memiliki pengetahuan dan kemampuan yang baik dalam menjelaskan metode yang digunakan dalam melakukan penilian risiko. Sehingga tidak ada kesalahpahaman dalam menerima informasi yang disampaikan oleh faslilitator pada pihak kami, jika ingin melakukan penelitian di perusahaan." **Wcr.inf01.MO.stat04**

Hasil wawancara pada narasumber menyatakan bahwa dalam melakukan penilian risiko untuk

menghasilkan konsistensi pemrioritasan risiko menggunakan metode FMEA. Cara yang dilakukan dengan memastikan kemampuan fasilitator FMEA dalam memberikan detail penjelasan dalam melakukan penilaian risiko hingga pemrioritasan risiko menggunakan FMEA dengan panduan yang jelas. Sehingga narasumber tidak terkejut dengan penilaian risiko menggunakan metode baru yang belum diterapkan pada perusahaan dalam melakukan penilaian risiko. Dan narasumber dapat dengan senang hati menerima ilmu baru dalam melakukan penilaian risiko perusahaan untuk menjadi perbandingan dalam melakukan penilaian risiko pada perusahaan.

4.7.7.2. Proposisi Mayor

Analisis risiko penggunaan teknologi informasi menggunakan metode FMEA pada perusahaan perbankan diperlukan suatu metode pemprioritasan yang telah disepakati oleh perusahaan. Dan adanya penggunaan prosedur yang telah ditetapkan sebagai panduan dalam melakukan penilaian risiko. Hal ini mengkonfirmasi pernyataan dari penggunaan pandungan Failure Mode and Effect Analysis (2008) mengenai Prosedur pada penggunaan metode dalam melakukan penilaian risiko memiliki batasan yang diambil untuk membuat kesepakatan dalam melakukan analisis, membuat rekomendasi perbaikan, pelaksanaan perbaikan, dll dalam melakukan penilaian risiko menggunakan metode FMEA. Dan pendapat dari Robillard mengenai adanya panduan untuk membimbing penggunaan pendekatan yang digunakan oleh perusahaan secara sistematis dalam melakukan manajemen risiko (Integrated Risk Management Framework, 2011).

Pemberian nilai risiko tidak hanya menjadi tanggung jawab bagi tim FMEA dalam melakukan

penilaian risiko, tetapi juga ada kerja sama baik dengan pihak yang bertanggung jawab pada penggunaan aset teknologi informasi yang akan dilakukan analisis risiko terkait dengan pengetahuan dan pengalaman yang dimiliki. Sehingga penilaian risiko tidak dilakukan secara subjektif, tetapi berdasarkan dokumen fakta evaluasi dan temuan audit pada aset teknologi informasi yang digunakan terkait dengan pemberian nilai risiko. Hal ini mendukung pernyataan Villacourt (1992) yang mengemukakan pendapatnya, Pengetahuan narasumber terhadap analisis penialaian risiko menggunakan metode FMEA juga berpengaruh pada performa tim FMEA dalam melakukan penilaian, apakah telah melakukan penilaian pada narasumber yang benar dan bertanggung jawab atas aset kritis yang dilakukan analisis risiko.

Kerja sama antara tim fasilitator FMEA dan narasumber sebagai pihak yang bertanggung jawab terhadap penggunaan aset teknologi informasi memiliki peran penting. Sehingga tim fasilitator FMEA dapat memiliki kemampuan komunikasi yang baik dan berpengalaman dalam membantu menyampaikan analisis penilaian risiko menggunakan metode FMEA. Hal ini mendukung pernyataan dari M.T. Oldenhofa (2011) mengenai konsistensi antara hasil FMEA dapat ditingkatkan dengan mengembangkan keterampilan sejumlah kecil fasilitator berpengalaman yang dapat membantu para analis untuk menggunakan FMEA lebih efektif dan konsisten dengan membantu dalam definisi mode kegagalan dan peringkat keparahan, probabilitas dan indeks pendeteksian.

Berdasarkan penelitian yang dilakukan ditemukan bahwa konsistensi penilaian risiko dipengaruhi oleh empat faktor yaitu: metode pemprioritasan risiko, prosedur penilaian risiko, pengetahuan narasumber, dan kemampuan fasilitator FMEA.

BAB V
FORMULASI KERANGKA FMEA YANG DISESUAIKAN

Bab ini menjelaskan sintesis kerangka kerja FMEA dilakukan untuk penyusunan modifikasi kerangka FMEA yang Disesuaikan untuk memberikan panduan dalam melakukan penilaian risiko sehingga mendapatkan hasil yang konsisten dari hasil penelitian yang dilakukan sebelumnya dalam mengetahui konsistensi penggunaan metode FMEA. Serta pada bab ini, dijelaskan mengenai pembahasan alur penggunaan kerangka FMEA yang Disesuaikan.

5.1. Modifikasi Kerangka FMEA : ASQ Automotive Division Webinar

ASQ Automative Division Webinar menggunakan metode FMEA yang digabungkan dengan referensi AIAG (*Automotive Industry Action Group*) FMEA dan menggunakan DFMEA (*Design FMEA*) dan PFMEA (*Process FMEA*) untuk memperkuat hasil analisis risiko menggunakan metode FMEA. Penelitian ini dilakukan oleh Mark A. Morris dalam Failure Mode and Effects Analysis based on FMEA 4th Edition (Morris, 2011). Tujuan dari penggunaan kerangka ini untuk menjelaskan tujuan, keuntungan, dan sasaran FMEA; memilih tim yang berkompeten untuk melakukan analisis risiko menggunakan FMEA, mengembangkan dan memenuhi FMEA, melakukan tinjauan, kritik, dan perbaruan dari FMEA yang telah ada, mengatur kegiatan tindak lanjut dan verifikasi dari penggunaan FMEA, mengembangkan FMEA yang sesuai dengan referensi AIAG FMEA.

Alur kerja yang penggunaan modifikasi kerangka FMEA yang dilakukan oleh ASQ Automotive Division Webinar sebagai berikut :

Gambar 5.1.1. Kerangka FMEA – ASQ Automotive Division (Sumber: Morris, 2011)

5.1.1. Menentukan Lingkup

Tahapan untuk menentukan lingkup sangat penting untuk menentukan batasan-batasan yang diperlukan dalam menggunakan metode FMEA, terkait dengan penggunaan beberapa dokumen untuk menentukan ruang lingkup penggunaan proses FMEA. Dokumen ini bisa berupa, *process flow diagram, relationship matrix, sketches,* dan *bill of materials* (BOM).

5.1.2. Menentukan Pelanggan

Analisis risiko yang dilakukan dari segi pelanggan seperti pengguna akhir, pemasok, lembaga pemerintah. Sehingga ada pengetahuan baru yang dapat digunakan sebagai referensi dalam melakukan analisis risiko terkait fungsi, persyaratan, dan spesifikasi yang diperlukan.

5.1.3. Mengidentifikasi Fungsi, Kebutuhan, dan Spesifikasi

Tahapan mengidentifikasi fungsi, kebutuhan, dan spesifikasi untuk mengidentifikasi langkah-langkah dari proses penggunaan metode FMEA, persyaratan yang dibutuhkan, hingga spesifikasi yang telah disesuaikan dengan ruang lingkup yang telah ditentukan. Sehingga maksud dan tujuan dari penilaian risiko menggunakan metode FMEA menjadi jelas.

5.1.4. Mengidentifikasi Potensi Penyebab

Potensi penyebab kegagalan untuk mengidentifikasi bagaimana kegagalan dapat terjadi yang seharusnya dapat dilakukan perbaikan dan pengendalian. Tujuan dari tahapan ini untuk menggambarkan hubungan antara sebab dan akibat dari potensi penyebab kegagalan yang mungkin terjadi.

5.1.5. Mengidentifikasi Potensi Dampak

Identifikasi potensi dampak bertujuan untuk mengetahui efek apa saja yang dihasilkan jika risiko tersebut terjadi.

Identifikasi potensi dampak yang terjadi ini dilakukan berdasarkan daftar potensi risiko yang telah diidentifikasi sebelumnya.

5.1.6. Mengidentifikasi Kontrol

Tahapan mengidentifikasi kontrol bertujuan untuk melakukan analisis terhadap proses kontrol yang telah dilakukan dalam mengantisipasi terjadinya risiko. Kontrol yang dilakukan terdapat dua jenis, yaitu kontrol preventif dan kontrol detektif. Kontrol preventif dilakukan dengan tujuan menghilangkan penyebab kegagalan atau mengurangi seberapa sering risiko mungkin terjadi. Dan kontrol detektif untuk mengenali penyebab kegagalan dan bagaiamanan cara melakukan tindakan penanggulangan.

5.1.7. Mengidentifikasi dan Memprioritaskan Risiko

Proses identifikasi risiko dilakukan dengan tiga cara, yaitu :

- *Severity* – untuk mengukur dampak dari risiko.
- *Occurence* – untuk menilai seberapa sering kemungkinan penyebab risiko dapat terjadi.
- *Detection* – untuk mengetahui kemampuan deteksi pada penyebab terjadinya risiko yang telah dilakukan.

Beberapa strategi untuk melakukan pemrioritasan risiko, yaitu dengan cara :

1). *High Risk Priority Numbers*
2). *Hight Severity Risks (berdasarkan RPN)*
3). *Hish Design Risks (Severity x Occurence)*
4). *Alternatif lainnya (S,O,D) dan (S,D)*

5.1.8. Membuat Rekomendasi

Rekomendasi dilakukan untuk mengurain terjadinya risiko dimana rekomendasi dibuat dapat berdasarkan dengan tujuan untuk mengurangi tingkat keparahan atau dampak dari risiko, mengurangi frekuensi kemungkinan terjadinya

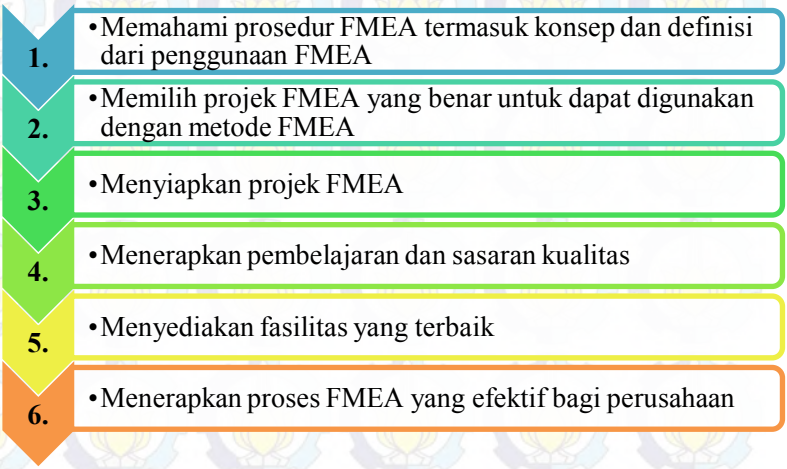
risiko, hingga memperbaikan deteksi untuk mencegah dan meminimalisir terjadinya risiko.

5.1.9. Verifikasi Hasil

Verifikasi hasil dilakukan untuk mengambil keputusan berdasarkan hasil dari penilaian risiko dan rekomendasi tindakan yang telah dibuat apakah mendapatkan persetujuan atau tidak. Serta untuk dilakukan peninjauan ulang terhadap tindakan-tindakan yang telah dilakukan.

5.2. Modifikasi Kerangka FMEA : *Understanding and Applying the Fundamentals of FMEAs*

Pemahaman dan penerapan fundamental FMEA yang dilakukan oleh Carl S. Carlson dari ReliaSoft Corporation dengan tujuan untuk memberikan penjelasan mengenai konsep dan prosedur penggunaan FMEA secara efektif dengan enam sukses faktor pada penggunaan FMEA (Carlson, 2014). Keenam sukses faktor yaitu :



Gambar 5.2.1. *Understanding and Applying the Fundamentals of FMEAs* (Sumber: Carlson, 2014)

5.2.1. Memahami prosedur FMEA termasuk konsep dan definisi dari penggunaan FMEA

FMEA adalah suatu metode untuk mengidentifikasi potensi kegagalan dan penyebab hingga dampak yang mungkin terjadi dari kegagalan sistem atau pengguna terakhir, dan dapat digunakan untuk menganalisis risiko pada suatu proses atau sistem yang dikembangkan. FMEA juga dapat digunakan untuk mengidentifikasi kekurangan suatu sistem sebelum diimplementasikan. Tujuan utama penggunaan FMEA adalah untuk memperbaiki rancangan suatu sistem dan memperbaiki rancangan sub-sistem atau komponen sistem (Carlson, 2014).

5.2.2. Memilih projek FMEA yang benar

Pemilihan projek yang akan dilakukan managemen risiko menggunakan FMEA, diperlukan pemilihan karena manajemen risiko yang akan dilakukan membutuhkan waktu dan uang, mampu melakukan analisis risiko secara efektif melalui penggunaan prosedur FMEA, penyediaan sumber daya manusia yang paham mengenai penggunaan metode FMEA. Sehingga, perusahaan dapat melakukan identifikasi kriteria sebelumnya untuk melakukan penilaian risiko menggunakan metode FMEA, seperti :

- Teknologi terbaru
- Rancangan baru dimana risiko menjadi perhatian
- Aplikasi baru pada teknologi yang telah ada
- Potensi pada persoalan keamanan
- Sejarah pada masalah yang signifikan
- Potensi pada persoalan regulasi penting
- Misi aplikasi kritis
- Kemampuan pemasok atau rekanan

Penggunaan kriteria dalam melakukan penilaian risiko dapat unik sesuai dengan kebutuhan perusahaan.

5.2.3. Menyiapkan projek FMEA

Persiapan untuk melakukan manajemen risiko menggunakan metode FMEA dapat menggunakan cara :

- Menentukan jangkauan pada proyek FMEA yang menjelaskan mengenai sistem, rancangan dan proses analisis risiko menggunakan FMEA.
- Membuat jangkauan yang dibuat nampak, dapat menggunakan tampilan matrix FMEA, parameter diagram, diagram blok fungsional.
- Membuat tim FMEA yang benar dimana terdiri dari tim yang merangcang analisis yang akan dilakukan menggunakan FMEA, pihak manajemen yang berwewenang, dan karyawan terkait.
- Menetapkan asumsi untuk melakukan analisis dan peraturan yang digunakan.
- Mengumpulkan informasi terkait konfigurasi sistem, gambaran, penilaian risiko terdahulu, sejarah, perencanaan tes, dan lain-lainnya.
- Menyiapkan pertemuan FMEA terkait dengan persiapan yang akan dilakukan, checklist yang akan digunakan dalam melakukan analisis risiko hingga mengalokasikan waktu secara efektif dan efisien.

5.2.4. Menerapkan pembelajaran dan sasaran kualitas

Tujuan untuk melakukan penerapan dari pembelajaran dan menggunakan sasaran kualitas ialah, untuk mendeteksi kesalahan yang mungkin terjadi terkait dengan penggunaan metode FMEA. Dua pernyataan yang digunakan untuk mengetahui kesalahan yang mungkin terjadi, yaitu:

- Apa yang menyebabkan penggunaan FMEA dapat melakukan kesalahan?

- Apa saja faktor yang menyebabkan penggunaan FMEA kurang efektif terkait dengan sasaran kualitas?

Cara yang dilakukan untuk untuk memperbaiki kualitas dalam melakukan penilaian risiko menggunakan metode FMEA dengan menggunakan cara :

1. *Design improvements*
2. *High risk failure modes*
3. *Control plan*
4. *Lessons's learned*
5. *Level of detail*
6. *Timing*
7. *Team*
8. *Documentation*
9. *Team*
10. *Documentation*
11. *Time usage*

5.2.5. Menyediakan fasilitator terbaik

Menyediakan fasilitator terlatih yang dapat membuat teknik yang efektif, menjalankan prosedur FMEA, dan mampu menentukan pilihan dalam penggunaan software yang sesuai. Tim yang melakukan analisis risiko adalah tim yang telah terlatih dan memahami konsep, pengertiaan, dan prosedur penggunaan FMEA. Karena dengan memberikan fasilitator terbaik dapat mencegah kegagalan risiko tinggi tanpa membuat waktu. Kemampuan yang dibutuhkan oleh fasilitator adalah :

- Brainstorming
- *Encouraging participation*
- *Active listening*
- *Controlling discussion*
- *Making decisions*
- *Conflict management*

- *Managing level of detail*
- *Managing time*
- *Unleashing team creativity*

5.2.6. Menerapkan proses FMEA yang efektif bagi perusahaan

Penerapan proses FMEA yang efektif mampu mendukung pengembangan sistem menjadi lebih handal dan pencapaian alokasi waktu yang tepat. Penerapan proses FMEA yang efektif mampu membuat kesepakatan efektif dalam membuat strategi, membantu dalam mengintegrasikan FMEA dengan proses bisnis lainnya, memberikan ulasan yang efektif dalam menangani kegagalan yang memiliki risiko tinggi dan membuat rekomendasi tindakan.

5.3. Modifikasi Kerangka FMEA : FMEA in Banking

Penggunaan FMEA dimulai pada tahun 1940an di Amerika Serikat pada bidang manufaktur. Kini, penggunaan FMEA juga digunakan pada industri perbankan. Bank membutuhkan pengembangan produk yang cepat dengan kualitas terbaik yang dapat meningkatkan kualitas dari loyalitas pelanggan. Kunci untuk meningkatkan pengembangan kualitas pada komponen produk dan kebutuhan bisnis yang membutuhkan pengujian prioritas tertinggi melalui penggunaan metode FMEA (Gundry, 2014).

Gambar 5.3.1. Kerangka FMEA in Banking
(Sumber: Gundry, 2014)

5.3.1. Proses FMEA

Pada tahapan proses FMEA terdiri dari::

- Mengidentifikasi potensi kegagalan untuk menghasilkan daftar risiko yang mungkin.
- Mengidentifikasi potensi penyebab dari setiap kegagalan untuk menghasilkan analisis terhadap risiko kegagalan yang mungkin terjadi.
- Mengidentifikasi dampak dari kegagalan yang terjadi untuk menghasilkan analisis dalam melakukan penilaian *severity*.

- Mengidentifikasi kemungkinan terjadi kegagalan untuk menghasilkan analisis dalam melakukan penilaian *occurency*.
- Menilai kontrol yang dilakukan untuk mendeteksi penyebab kegagalan untuk menghasilkan analisis dalam melakukan penilaian *detection*.

5.3.2. Memfasilitasi Proses FMEA

Tahapan memfasilitasi proses FMEA terdiri dari beberapa tahapan, yaitu:

- Menentukan siapa yang berpartisipasi dalam melakukan penilaian risiko menggunakan FMEA dimana tim yang melakukan penilaian risiko menggunakan metode FMEA ini telah memahami seluruh proses FMEA.
- Memastikan pihak yang terlibat dalam penilaian bersikap jujur terhadap poin penilaian
- Menyediakan template dokumen penunjang yang memudahkan dalam melakukan penilaian risiko
- Memandu jalannya penggunaan FMEA

5.4. Sintesis Kerangka FMEA yang Disesuaikan

Sintesis Kerangka FMEA yang Disesuaikan dilakukan dengan cara melakukan kajian penelitian yang pernah dilakukan sebelumnya terkait dengan modifikasi kerangka FMEA, yaitu penelitian pada Modifikasi FMEA – ASQ Automotive Division Webinar, *Undertansing and Applying the Fundamentals of FMEAs, FMEA in Banking*.

Tabel 5.4.1. Tahapan pada Penelitian Modifikasi FMEA: ASQ Automotive Division Webinar, Understanding and Applying the Fundamentals of FMEAs, FMEA in Banking (Sumber: Peneliti, 2014)

Tahapan Analisis Risiko	***FMEA - ASQ Automotive Division Webinar*** (Morris, 2011)	***Understanding and Applying the Fundamentals of FMEA*** (Carlson, 2014)	***FMEA in Banking*** (Gundry, 2014)
1	Menentukan Jangkauan	Memahami prosedur FMEA termasuk konsep dan definisi dari penggunaan FMEA	Mengidentifkasi potensi kegagalan (Proses FMEA)
2	Menentukan Pelanggan	Memilih projek FMEA yang benar untuk dapat digunakan dengan metode FMEA	Mengidentifikasi potensi penyebab dari setiap kegagalan (Proses FMEA)
3	Mengidentifikasi Fungsi, Kebutuhan, dan Spesifikasi	Menyiapkan projek FMEA	Menilai dampak dari kegagalan yang terjadi (Proses FMEA)
4	Mengidentifikasi Potensi Kegagalan	Menerapkan pembelajaran dan sasaran kualitas	Menilai kemungkinan terjadi kegagalan (Proses FMEA)
5	Mengidentifikasi Potensi Penyebab	Menyediakan fasilitas terbaik	Menilai kontrol yang telah dilakukan untuk mendeteksi penyebab kegagalan (Proses FMEA)
6	Mengidentifikasi Potensi Dampak	Menerapkan proses FMEA yang efektif bagi perusahaan	Menentukan siapa yang berpartisipasi (Memfasilitasi proses FMEA)
7	Mengidentifikasi Kontrol		Memastikan pihak yang terlibat dalam penilaian (Memfasilitasi proses FMEA)

Tahapan Analisis Risiko	*FMEA - ASQ Automotive Division Webinar* (Morris, 2011)	*Understanding and Applying the Fundamentals of FMEA* (Carlson, 2014)	*FMEA in Banking* (Gundry, 2014)
8	Mengidentifikasi dan Memprioritaskan Risiko		Menyediakan template dokumen penunjang (Memfasilitasi proses FMEA)
9	Membuat Rekomendasi		Memandu jalannya penggunaan FMEA (Memfasilitasi proses FMEA)
10	Verifikasi Hasil		

Pada kajian literatur penelitian modifikasi FMEA dapat dilihat langkah-langkah yang digunakan dalam melakukan penilaian risiko. Tiga penelitian di atas memiliki kelebihan dan kekurangan pada setiap tahapan dan sudut pandang yang digunakan.

Tabel 5.4.2. Kelemahan dan Kelebihan pada setiap penelitian pada FMEA: ASQ Automotive Division Webinar, Understanding and Applying the Fundamentals of FMEAs, FMEA in Banking (Sumber: Peneliti, 2014)

	FMEA - ASQ Automotive Division Webinar (Morris, 2011)	*Understanding and Applying the Fundamentals of FMEA* (Carlson, 2014)	*FMEA in Banking* (Gundry, 2014)
Kelemahan	• Belum adanya panduan untuk pemilihan pihak yang sesuai kriteria untuk melakukan penilaian risiko.	• Belum adanya penjelasan secara detail mengenai cara melakukan tahapan efektivitas penerapan	• Belum adanya tahapan untuk melakukan tindakan selanjutnya setelah melakukan

		FMEA.	penilaian risiko.
Kelebihan	• Adanya tahapan untuk menentukan tujuan, keuntungan, dan sasaran dari penggunaan FMEA • Melakukan tinjauan, kritik, dan perbaruan dari FMEA yang telah ada • Mengatur kegiatan tindak lanjut dan verifikasi dari penggunaan FMEA	• Memberikan penjelasan mengenai konsep dan prosedur penggunaan FMEA secara efektif dengan enam sukses faktor. • Menjelaskan langkah-langkah secara detail pada setiap faktor pada enam sukses faktor yang diterapkan.	• Adanya tahapan untuk melakukan identifikasi potensi kegagalan dan identifikasi potensi penyebab dari setiap kegagalan secara detail

Analisis kelebihan dan kekurangan dari ketiga penelitian, FMEA (ASQ Automotive Division Webinar, *Understanding and Applying the Fundamentals of FMEA,* dan *FMEA in Banking*), dijadikan panduan untuk membuat Formulasi FMEA yang Disesuaikan. Pembuatan formulasi ini berdasarkan kebutuhan perusahaan XYZ untuk meningkatkan konsistensi hasil penilaian risiko menggunakan metode FMEA. Pada tabel 6.4.2 dilakukan pemetaan ketiga metode penelitian modifikasi FMEA berdasarkan kesamaan tahapan yang digunakan dalam melakukan penilian risiko untuk membuat kerangka FMEA yang Disesuaikan.

Tabel 5.4.3. Pemetaan Kerangka FMEA yang Disesuaikan dengan Panduan Penelitian Sebelumnya (Sumber: Peneliti, 2014)

FASE	SUB-FASE	ACUAN
Preparation **(Persiapan)**	Memahami Prosedur	***Understanding and Applying the Fundamentals of FMEA*** (Carlson, 2014)
	Menerapkan Pembelajaran	***Understanding and Applying the Fundamentals of FMEA*** (Carlson, 2014)
	Menentukan Penyeragaman Metode Penilaian	***Understanding and Applying the Fundamentals of FMEA*** (Carlson, 2014)
	Menentukan Pihak yang Berpartisipasi	***Understanding and Applying the Fundamentals of FMEA*** (Carlson, 2014)
Risk Analyze **(Analisis Risiko)**	Mengidentifikasi Aset Kritis	***FMEA - ASQ Automotive Division Webinar*** (Morris, 2011)
	Brainstorm Potensi Kegagalan	***FMEA - ASQ Automotive Division Webinar*** (Morris, 2011)
Risk Scoring **(Penilaian Risiko)**	Menilai Dampak Risiko	***FMEA in Banking*** (Gundry, 2014)
	Menilai Frekuensi Kemungkinan Risiko	***FMEA in Banking*** (Gundry, 2014)
	Menilai Deteksi Risiko	***FMEA in Banking*** (Gundry, 2014)
Risk Priority **(Prioritas Risiko)**	Menghitung Risk Priority Number (RPN)	***FMEA in Banking*** (Gundry, 2014)
Check and Action **(Cek dan Lakukan)**	Membuat Rekomendasi Kontrol	***FMEA - ASQ Automotive Division Webinar*** (Morris, 2011)
	Verifikasi Hasil	***FMEA - ASQ Automotive Division Webinar*** (Morris, 2011)

5.5. Alasan Pemilihan Sub Fase Formulasi Kerangka FMEA yang Disesuaikan

Pembuatan formulasi Kerangka FMEA yang Disesuaikan berdasarkan hasil sintesi penelitian terdahulu dan dalam menentukan setiap sub-fase untuk merancang Kerangka FMEA yang Disesuaikan memiliki alasan.

Tabel 5.5.1. Alasan Pemilihan Sub Fase Formulasi Kerangka FMEA yang Disesuaikan (Sumber: Peneliti, 2014)

FASE	SUB-FASE	ACUAN
Preparation **(Persiapan)**	Memahami Prosedur	*Understanding and Applying the Fundamentals of FMEA* (Carlson, 2014), kerangka ini memiliki tahapan yang menjelaskan bagaiaman proses dalam melakukan pemahaman prosedur penggunaan metode FMEA. Sehingga semua pihak yang terlibat telah memahami penggunaan FMEA sesuai dengan prosedur yang telah dibuat untuk mengurangi kesalahan dan perbedaan hasil dalam melakukan penilaian risiko menggunakan metode FMEA
	Menerapkan Pembelajaran	*Understanding and Applying the Fundamentals of FMEA* (Carlson, 2014), memiliki tahapan untuk menerapkan pembelajaran dan sasaran kualitas terkait untuk memperbaiki kualitas dalam melakukan penilaian risiko. Penilaian risiko didasarkan pada dokumen terdahulu yang sudah pernah dibuat yang ada kaitannya dengan analisis risiko, salah satunya dokumen hasil audit, dapat juga dengan melihat

		dokumen kontrol yang telah dibuat, dan segala aktivitas lainnya yang dapat menunjang proses analisis risiko yang dapat dijadikan acuan dalam melakukan penilaian risiko. Sehingga menghindari penilaian risiko yang bersifat subjektif.
	Menentukan Penyeragaman Metode Penilaian	*Understanding and Applying the Fundamentals of FMEA* (Carlson, 2014), tahapan pendukung untuk menentukan penyeragaman metode penilian pada kerangka ini, yaitu adanya tahapan untuk melakukan persiapan proyek. Cara yang dilakukan adalah dengan menentukan ruang lingkup penilaian risiko, dalam hal ini dapat berkaitan dengan menentukan ruang lingkup dengan tujuan untuk menyeragamkan metode yang digunakan dalam melakukan penilaian risiko menggunakan metode FMEA, mulai dari skala penilaian, jumlah batasan risiko tertinggi, dan lainnya.
	Menentukan Pihak yang Berpartisipasi	*Understanding and Applying the Fundamentals of FMEA* (Carlson, 2014), menentukan pihak yang berpartisipasi didukung pada penggunaan kerangka ini yang telah menyajikan tahap untuk menyediakan fasilitator terbaik. Seorang fasilitator FMEA memiliki kemampuan dalam memahami konsep, pengertian, pelatihan, hingga kemampuan

		dalam menggunakan metode ini, serta telah mengikuti pelatihan. Sehingga, harapannya dengan menentukan fasilitator terbaik dapat menggali kemampuan fasilitator dalam melakukan *brainstorming*, mengambil keputusan, melakukan manajemen terbaik dalam tim, dan kemampuan lainnya yang berkaitan dengan aktivitas penilaian risiko menggunakan metode FMEA.
Risk Analyze **(Analisis Risiko)**	Mengidentifikasi Aset Kritis	*FMEA - ASQ Automotive Division Webinar* (Morris, 2011), sub fase dalam melakukan identifikasi aset kritis diterapkan pada kerangka ini pada tahapan mengidentifikasi fungsi, kebutuhan, dan spesifikasi sebelum tahapan melakukan identifikasi potensi kegagalan yang mungkin terjadi.
	Brainstorm Potensi Kegagalan	*FMEA - ASQ Automotive Division Webinar* (Morris, 2011), melakukan tahapan untuk mengidentifikasi potensi kegagalan yang tidak hanya berasal dari sudut pandang karyawan saja, tetapi melibatkan pihak lain, seperti pelanggan, pengguna akhir, hingga kebijakan pemerintah untuk mengidentifikasi risiko secara mendalam,
Risk Scoring **(Penilaian Risiko)**	Menilai Dampak Risiko	*FMEA in Banking* (Gundry, 2014), melakukan analisis dampak risiko yang terjadi sesuai dengan sudut pandang pada kondisi perbankan yang sesuai

		dengan studi kasus penelitian ini.
	Menilai Frekuensi Kemungkinan Risiko	*FMEA in Banking* (Gundry, 2014), melakukan analisis frekuensi risiko terjadi sesuai dengan sudut pandang pada kondisi perbankan yang sesuai dengan studi kasus penelitian ini.
	Menilai Deteksi Risiko	*FMEA in Banking* (Gundry, 2014), melakukan analisis deteksi pada risiko yang telah dilakukan oleh perusahaan sesuai dengan sudut pandang pada kondisi perbankan yang sesuai dengan studi kasus penelitian ini.
***Risk Priority* (Prioritas Risiko)**	Menghitung Risk Priority Number (RPN)	*FMEA in Banking* (Gundry, 2014), perhitungan RPN didasarkan pada kerangka FMEA in Banking untuk mendukung penelitian dalam penggunaan metode FMEA untuk melakukan penilian risiko di perusahaan perbankan.
***Check and Action* (Cek dan Lakukan)**	Membuat Rekomendasi Kontrol	*FMEA - ASQ Automotive Division Webinar* (Morris, 2011), kerangka ini memiliki detail analisis dalam melakukan rekomendasi kontrol yang lengkap dengan mempertimbangkan kontrol yang telah dilakukan dari segi kontrol perpektif dan kontrol detektif.
	Verifikasi Hasil	*FMEA - ASQ Automotive Division Webinar* (Morris, 2011), kerangka ini mampu memberikan detail mengenai tahapan bagaimana cara melakukan verifikasi hasil secara efektif.

5.6. Formulasi Kerangka FMEA yang Disesuaikan

Hasil pemetaan risiko Kerangka FMEA yang Disesuaikan, dipetakan dari empat hasil penyebab penilaian risiko menggunakan metode FMEA tidak konsisten dengan menggunakan metode penilitian kualitatif, yaitu prosedur, metode yang digunakan, pihak narasumber dan fasilitator. Kemudian dilakukan sistesis dari penelitian terdahalu yang melakukan modifikasi pada kerangka FMEA pada kerangka FMEA pada ASQ Automotive Division Webinar, *Understanding and Applying the Fundamentals of FMEA,* dan *FMEA in Banking*. Maka, penelitian menghasilkan ramuan langkah-langkah melakukan manajemen risiko menggunakan metode FMEA untuk menghasilkan penilaian yang konsisten.

Gambar 5.6.1. Formulasi Kerangka FMEA yang Disesuaikan
(Sumber: Olahan Peneliti, 2014)

5.7. Penjelasan Alur Kerangka FMEA yang Disesuaikan

Penjelasan alur Kerangka FMEA yang Disesuaikan sebagai petunjuk penggunaan. Pada Kerangka FMEA yang Disesuaikan dibagi mejadi lima tahapan, yaitu tahapan Persiapan, Analisis Risiko, Penilaian Risiko, Prioritas Risiko, Cek dan Lakukan.

5.7.1 *Preparation* (Persiapan)

Tahapan perencanaan berisikan beberapa langkah tahapan untuk mendukung proses sebelum melakukan analisis dan penilaian risiko menggunakan metode FMEA. Tahapan persiapan dilakukan oleh seluruh pihak yang berkaitan dengan kegiatan dalam melakukan analisis risiko terutama tim yang akan melakukan analisis risiko.

1. **Memahami Prosedur**
   Adanya prosedur yang dibuat oleh perusahaan terkait dengan penilaian risiko menggunakan metode FMEA untuk mengurangi ketidakonsistenan pada hasil penilaian risiko. Prosedur digunakan untuk menjelaskan detail langkah-langkah yang perlu dilakukan dalam menganalisis dan menilai risiko menggunakan metode FMEA.
2. **Menerapkan Pembelajaran Dokumen Audit**
   Pada tahapan penerapan pembelajaran dokumen evaluasi dilakukan dengan tujuan untuk mengetahui hasil dari dokumen audit yang telah dilakukan oleh perusahaan, yang dapat digunakan sebagai acuan dalam melakukan analisis risiko dan pemberian nilai risiko agar terhindar dari subjektivitas atau persepsi tim atau orang yang melakukan penilaian risiko. Sehingga penilaian risiko yang dihasilkan berdasarkan dengan kondisi dan fakta yang didapatkan dari dokumen audit, bukan subjektivitas penilai.

3. **Menentukan Metode yang Digunakan untuk Penilaian**

Tahapan yang dilakukan untuk menentukan metode yang digunakan untuk melakukan penilaian dengan tujuan menyamakan persepsi dari hasil kesepakatan yang telah dibuat oleh perusahaan. Sehingga metode melakukan penilaian menggunakan metode FMEA memberikan hasil yang konsisten walaupun dilakukan oleh tim yang berbeda. Karena telah berdasarkan prosedur untuk menentukan metode yang disepakati. Pemilihan metode yang digunakan, salah satunya dengan menyamakan kesepakatan sesuai dengan kebijakan perusahaan untuk menentukan jumlah risiko yang memiliki level tertinggi. Dan, metode untuk skala penilaian untuk memberikan penilaian risiko pada dampak, kemungkinan, dan deteksi. Pada penelitian ini, skala penilaian yang digunakan ialah skala 1-10:

Petunjuk Pemberian Nilai Dampak (*Severity* = S)

Petunjuk pemberian skor pada kategori *Severity (Impact)* bertujuan untuk melihat dampak atau pengaruh besar risiko terhadap aspek-aspek tujuan proyek, meliputi jadwal *(timeline),* biaya (*cost*) dan teknikal (*technical / operational*), Skala yang digunakan adalah 1-10 dimana nilai 1 memiliki dampak yang tidak memiliki efek terhadap risiko yang terjadi hingga nilai 10 yang berarti dampak dari risiko tersebut adalah memiliki dampak yang besar yang berpengaruh pada proses bisnis perusahaan. Arti dari pemberian nilai dampak risiko, semakin tinggi nilai dampak risiko yang diberikan maka dampak yang terjadi semakin besar dapat mengganggu keberlangusngan proses bisnis perusahaan.

Tabel 5.7.1.1. Nilai Dampak (Sumber: FMEA)

Effect	*Severity of Effect*	*Ranking*
Hazardous: without warning	Potensial kegagalan atau risiko mempengaruhi keamanan sistem tanpa peringatan	10
Hazardous: with warning	Potensial kegagalan atau risiko mempengaruhi keamanan sistem dengan peringatan	9
Very high	Tidak dapat dioperasikan dengan kegagalan yang merusak tanpa mengorbankan keamanan	8
High	Tidak dapat dioperasikan dengan kerugian atau kerusakan peralatan	7
Moderate	Tidak dapat dioperasikan dengan kerugian kecil (Proses)	6
Low	Tidak dapat dioperasikan tanpa kerugian (Prosedur)	5
Very Low	Penurunan Kinerja secara signifikan (*Policy*)	4
Minor	Penurunan Kinerja	3
Very Minor	Efeknya kecil	2
None	Tidak memiliki efek	1

Petunjuk Pemberian Nilai Kemungkinan (*Occurence*=O)

Petunjuk pemberian skor pada kategori *Occurance (Likelihood)* bertujuan untuk mengidentifikasi kemungkinan terjadinya sebuah risiko. Skala yang digunakan adalah 1-10 dimana nilai 1 frekuensi kemungkinan terjadi risiko sangat kecil dan semakin tinggi nilai kemungkinan risiko terjadi, maka frekuensi risiko yang mungkin terjadi adalah semakin sering. Sehingga pemberian nilai 10 pada kemungkinan risiko yang memiliki kemungkinan terjadi lebih dari 1 kali terjadi setiap harinya.

Tabel 5.7.1.2. Nilai Kemungkinan (Sumber: FMEA)

Probability of Failure	***Possible Failure Rate***	***Ranking***
Very High: Failure is almost ineviTabel	Lebih dari 1 kali terjadi setiap harinya	10
High: Failures occur almost as often as not	1 kali terjadi setiap tiga hingga empat hari	9
High: Repeated Failures	1 kali terjadi setiap minggu	8
High: Failures occur often	1 kali terjadi setiap bulan	7
Moderately High: Frequent Failure	1 kali terjadi setiap tiga bulan	6
Moderately: Kadang-kadang kegagalan	1 kali terjadi setiap enam bulan	5
Moderately Low: Infrequent Failure	1 kali terjadi setiap tahun	4
Low: Relatively few failures	1 kali terjadi setiap satu hingga tiga tahun	3

Probability of Failure	*Possible Failure Rate*	*Ranking*
Low: Relatively few failures and far between	1 kali terjadi setiap tiga tahun hingga lima tahun	2
Remote: failure is unlikely	1 kali terjadi lebih dari lima tahun	1

Petunjuk Pemberian Nilai Deteksi (*Detection* = D)

Petunjuk pemberian skor pada kategori *Detection* bertujuan untuk mengukur tingkat efektivitas metode atau kemampuan untuk mendeteksi terjadinya suatu risiko. Deteksi dilakukan untuk melihat bagaiamana cara mendeteksi peristiwa yang memiliki risiko secara tepat, agar perusahaan mampu membuat tindakan terhadap risiko yang terdeteksi secara cepat. Pemberian nilai 1-10 dimana nilai 1 memiliki deteksi yang baik untuk mendeteksi risiko yang mungkin terjadi hingga nilai 10 dimana risiko belum dilakukan deteksi yang baik untuk mencegah terjadi risiko yang mungkin terjadi.

Tabel 5.7.1.3. Nilai Deteksi (Sumber: FMEA)

Detection	*Criteria: Likelihood of Detection*	*Ranking*
Absolutely Uncertainty	Kekurangan tidak dapat di deteksi penyebabnya	10
Very Remote	Melakukan sample atau pemeriksaan untuk mencek cacat atau kekurangan	9
Remote	Produk diterima berdasarkan ketidakcacatan dalam sample	8
Very Low	Semua produk diperiksa secara manual dalam proses	7

Detection	*Criteria: Likelihood of Detection*	*Ranking*
Low	Produk diinspeksi manual menggunakan mistake-proofing modification	6
Moderate	SPC (Statistical Process Control) digunakan dalam proses dan produk adalah final inspeksi	5
Moderately High	Kemampuan alat kontrol untuk mendeteksi bentuk dan penyebab kegagalan sedang sampai tinggi	4
High	Kemampuan alat kontrol untuk mendeteksi bentuk dan penyebab kegagalan tinggi	3
Very High	Semua produk secara otomatis diperiksa	2
Almost Certain	Kekurangan atau kecacatan sudah jelas dan dapat dicegah dari customer	1

4. Menentukan Pihak yang Berpartisipasi

Pihak yang berpartisipasi dalam melakukan penilaian risiko menggunakan metode FMEA adalah orang yang telah dibekali oleh dengan pelatihan dalam melakukan manajemen risiko terutama penilaian risiko menggunakan metode FMEA dan memiliki posisi dan tanggung jawab penting di perusahaan. Perusahaan Bank XYZ dalam menentukan pihak yang berpartisipasi dalam melakukan penilaian risiko dilakukan oleh Manajer Operasional terkait dengan penilaian risiko penggunaan teknologi informasi pada teller Bank XYZ. Manajer Operasional Bank XYZ mengetahui dan memahami dengan jelas kondisi lapangan, serta memiliki kemampuan untuk

melakukan penilaian risiko dan bertanggung jawab atas aset teknologi informasi pada teller Bank XYZ.

Kriteria pihak yang berpartisipasi pada penilaian risiko dilakukan oleh para *upper management* dalam studi kasus ini dilakukan oleh Manager Operasional Bank XYZ yang dibantu oleh fasilitator FMEA untuk menilai risiko menggunakan metode FMEA, dimana pihak penilaian memiliki kriteria, yaitu:

- **Memahami tujuan perusahaan dalam melakukan uji coba pada penggunaan aplikasi**, untuk memastikan bahwa perusahaan telah menerapkan analisis risiko untuk mencegah kemungkinan risiko yang terjadi pada investasi teknologi informasi yang telah dilakukan. Agar perusahaan tidak mengalami kerugian atas terjadinya risiko dari penggunaan teknologi informasi yang bertujuan untuk mendukung proses bisnis perusahaan menjadi lebih cepat, efektif, dan efisien.
- **Memahami proses bisnis perusahaan**, dari pihak Manager Operasional mampu menjelaskan secara detail mengenai proses bisnis perusahaan. Dan dari pihak fasilitator FMEA, mampu memahami dan mengamati proses bisnis yang terjadi pada perusahaan terkait terutama pada proses bisnis yang akan dilakukan analisis risiko, pada penggunaan teknologi informasi teller Bank XYZ.
- **Mampu membuat skenario uji coba**, untuk mengetahui kemungkinan risiko apa saja yang mungkin terjadi pada penggunaan teknologi informasi di perusahaan untuk menganalisis penyebab risiko, dampak dari risiko, kemungkinan risiko terjadi, hingga deteksi terhadap risiko yang telah dilakukan oleh

perusahaan. Sehingga memudahkan dalam mendapakan hasil analisis risiko pada setiap aset kritis pada penggunaan teknologi informasi pada teller Bank XYZ.

- **Memahami konsep penilaian risiko menggunakan metode FMEA**, pihak penilai adalah tim FMEA untuk melakukan analisis dan penilaian risiko. Sehingga setiap pihak memahami cara memberikan penilaian risiko berdasarkan dampak risiko, kemungkinan terjadi risiko, hingga deteksi terhadap risiko sesuai dengan skala pemberian nilai yang telah disepakati oleh perusahaan. Skala nilai yang ditetapkan untuk menganalisis risiko pada penggunaan teknologi informasi Bank XYZ adalah 1-10. Tiap nilai *severity, occurency*, dan *detection* akan menghasilkan nilai *Risk Priority Number* untuk menghasilkan risiko tetinggi yang membutuhkan perhatian dan urgensi tinggi untuk segera diberikan penanganan untuk mencegah risiko terjadi.

5.7.2 *Risk Analyze* (Analisis Risiko)

Analisis risiko adalah aspek krusial dalam melakukan managemen tes. Apa itu Analisis Risiko? Dan kenapa analisis risiko itu penting?

Risiko adalah kemungkinanan terjadinya sesuatu hal yang negatif pada suatu kejadian. Jika risiko tidak dapat diatasi dan diatur, maka hal ini dapat berdampak pada penurunan kinerja perusahaan hingga mengakibatkan ketidakpuasaan pelanggan. Pada penelitian, analisis risiko pada penggunaan teknologi informasi pada Bank XYZ diperlukan untuk memastikan bahwa penggunaan teknologi informasi dapat berjalan dengan lancar sehingga dapat diketahui risiko yang

mungkin terjadi dan kemudian dibuat penanganan dan pencegahan untuk meminimalisir terjadinya risiko yang tidak diinginkan. Karena kegagalan pada pengendalian dan pencegahan risiko dapat berpengaruh pada proses bisnis perusahaan dan ketidakpuasan nasabah yang dapat mengakibatkan kehilangan nasabah. Cara yang dilakukan dalam analisis risiko, yaitu:

1. **Mengidentifikasi Aset Kritis**

   Identifikasi aset kritis pada penggunaan teknologi informasi pada teller Bank XYZ adalah tahapan untuk mengetahui aset apa saja yang digunakan untuk memastikan keberlangsungan bisnis berjalan dengan lancar. Aset kritis yang diidentifikasi dapat dibedakan berdasarkan kategori aset kritis, yaitu: kategori informasi, hardware, software, dan sumber daya manusia. Dan pada identifikasi aset kritis ditambahkan identifikasi ancaman internal dan ancaman eksternal. Identifikasi aset kritis dapat memudahkan untuk melakukan tahapan selanjutnya dalam melakukan penggalian pada potensi kegagalan pada setiap aset kritis yang ada.

Tabel 5.7.2.1. Identifikasi Aset Kritis (Sumber: Peneliti, 2014)

Kategori Aset Kritis	Aset Kritis	Ancaman	
		Internal	Eksternal
<Berisikan kategori aset kritis berdasarkan jenis aset, yaitu kategoris informasi,hardware, software, dan sumber daya manusia>	*<Berisikan hasil identifikasi aset kritis pada penggunaan teknologi informasi teller Bank XYZ>*	*<Berisikan hasil identifikasi ancaman internal pada aset kritis Bank XYZ>*	*<Berisikan hasil identifikasi ancaman eksternal pada aset kritis Bank XYZ>*

2. **Brainstorm Potensi Kegagalan**

   Hasil daftar aset kritis yang telah dilakukan pada tahapan identifikasi aset kritis. Selanjutnya, daftar aset kritis yang ada dilakukan penggalian potensi kegagalan pada setiap aset kritis yaitu risiko yang mungkin terjadi pada

penggunaan aset kritis yang telah diidentifikasi. Potensi kegagalan menjelaskan bagaiaman proses kegagalan dapat terjadi, dimana dapat dilakukan kontrol dan koreksi pada setiap potensi kegagalan. Potensi kegagalan menghasilkan daftar risiko yang pada penggunaan aset kritis yang kemudian dilakukan identifikasi penyebab yang mungkin terjadi terhadap tiap risiko yang telah diidentifikasi. Tujuan dari identifikasi potensi kegagalan untuk menjelaskan keterkaitan antara penyebab dan hasil potensi kegagalan.

Tabel 5.7.2.2. Brainstorm Potensi Kegagalan (Sumber: Peneliti, 2014)

Kode	Kategori Aset Kritis	Risiko	Penyebab
<Pena-maan Kode Risiko>	*<Nama Kategori Aset Kritis>*	*<Risiko yang mungkin terjadi terhadap penggunaan aset kritis>*	*<Penyebab risiko terhadap penggunaan aset kritis>*

5.7.3 *Risk Scoring* (Penilaian Risiko)

Tahapan penilaian risiko menggunakan metode FMEA dibagi menjadi tiga kategori penilaian untuk mendapatkan nilai pada dampak risiko (*Severity*), nilai pada frekuensi kemungkinanan terjadi risiko (*Occurance*), dan nilai pada deteksi risiko (*detection*). Penilaian yang dilakukan menggunakan metode FMEA ini dapat menggunakan referensi dari dokumen audit untuk menghindari subjektivitas dalam memberikan nilai pada risiko. Sehingga hasil yang didapatkan berdasarkan kondisi perusahaan yang nyata, bukan hanya persepsi dari tim penilai.

1. **Menilai Dampak Risiko**

   Nilai dampak risiko diberikan untuk mengetahui hasil dari seberapa besar efek yang akan ditimbulkan jika

kegagalan risiko terjadi terhadap proses bisnis perusahaan. Sehingga dilakukan analisis dampak dari risiko yang ditimbulkan, kemudian diberikan penilaian.

Tabel 5.7.3.1. Penilaian Dampak Risiko - *Severity* (Sumber : Peneliti, 2014)

Kode	Risiko	Nilai *Severity*	Penjelasan Nilai	Alasan Pemberian Nilai
<Penamaan Kode Risiko>	*<Identifikasi risiko aset kritis>*	*<Pemberian nilai severity>*	*<Penjelasan nilai yang mengacu pada pemberian nilai FMEA>*	*<Alasan pemberian nilai yang mendukung penilaian, berdasarkan kondisi dan fakta perusahaan>*

2. Menilai Frekuensi Kemungkinan Risiko Terjadi

Nilai kemungkinan risiko diberikan untuk mengetahui hasil dari seberapa sering kemungkinan risiko akan terjadi. Sehingga dilakukan analisis pada kemungkinan terjadi risiko, kemudian diberikan penilaian.

Tabel 5.7.3.2. Penilaian Kemungkinan Risiko – *Occurence* (Sumber: Peneliti, 2014)

Kode	Risiko	Nilai *Occurance*	Penjelasan Nilai	Alasan Pemberian Nilai
<Penamaan Kode Risiko>	*<Identifikasi risiko aset kritis>*	*<Pemberian nilai occurence>*	*<Penjelasan nilai yang mengacu pada pemberian nilai FMEA>*	*<Alasan pemberian nilai yang mendukung penilaian, berdasarkan kondisi dan fakta perusahaan>*

3. Menilai Deteksi Risiko

Nilai deteksi risiko diberikan untuk mengetahui usaha yang dilakukan dalam mendeteksi terjadinya risiko yang tidak diinginkan. Sehingga dilakukan analisis pada deteksi risiko, kemudian diberikan penilaian.

Tabel 5.7.3.3. Penelian Deteksi Risiko – *Detection* (Sumber: Peneliti, 2014)

Kode	Risiko	Nilai *Detection*	Penjelasan Nilai	Alasan Pemberian Nilai
<Penamaan Kode Risiko>	*<Identifikasi risiko aset kritis>*	*<Pemberian nilai detection>*	*<Penjelasan nilai yang mengacu pada pemberian nilai FMEA>*	*<Alasan pemberian nilai yang mendukung penilaian, berdasarkan kondisi dan fakta perusahaan>*

5.7.4 *Risk Priority* (Prioritas Risiko)

Prioritas risiko didapatkan dari penggabungan nilai *severity, occurence,* dan *detection* menggunakan rumus (*Risk Priority Number*) RPN pada metode FMEA. Tujuan dari prioritas risiko untuk mengetahui risiko tertinggi yang membutuhkan perhatiaan dan tingkat urgensi tinggi untuk dilakukan kontrol dan kelola terhadap risiko tertinggi.

1. **Menghitung *Risk Priority Number* (RPN)**

   Cara melakukan perhitungan RPN dengan melakukan perkalian pada hasil nilai *severity (S), occurency* (*O*), dan *detection (D)*.

   $$RPN = S \times O \times D$$

   Hasil dari nilai RPN kemudian dikategorikan untuk menghasilkan prioritas risiko tertinggi hingga terendah, dengan cara melakukan pengkategorian berdasarkan level risiko:

Tabel 5.7.4.1. Pengkatogorian Level Risiko (Sumber: FMEA)

Level Risiko	Skala Nilai RPN
Very low	x < 20
Low	20≤ x <80
Medium	80≤ x <120
High	120≤ x <200
Very high	x>200

Pengkategorian level risiko berdasarkan hasil RPN dari tiap nilai risiko, hasil nilai RPN terendah memiliki skala di bawah 20, skala rendah 20-80, skala medium 80-120, skala tinggi 120-200, hingga skala tertinggi di atas 200.

5.7.5 *Check and Action* (Cek dan Lakukan)

Cara melakukan tahapan *check and action*, yaitu dengan cara menjalankan seluruh proses dari tahapan persiapan hingga pemrioritasan risiko. Kemudian dibuatlah rekomendasi kontrol, untuk membuat rekomendasi kontrol dapat menggunakan panduan ISO 27002 tentang Keamanan Informasi.

1. **Membuat Rekomendasi Kontrol**

   Pembuatan rekomendasi kontrol bertujuan untuk menghasilkan analisis untuk penanganan yang dapat dilakukan oleh perusahaan mencegah terjadinya risiko. Salah satu panduan yang dapat digunakan untuk membantu pembuatan kontrol risiko dalam menggunakan panduan ISO 27002 tentang teknik dalam melakukan Managemen Keamanan Informasi. Penggunaan panduan dalam melakukan risiko tidak hanya terbatas pada penggunaan ISO 27002, tetapi dapat menggunakan panduan kontrol risiko lainnya.

Tabel 5.7.5.1. Tabel Rekomendasi Kontrol (Sumber: Peneliti, 2014)

Kode	Risiko	Penyebab	Tindakan	Kontrol berdasarkan ISO 27002	Pihak yang Bertanggung Jawab
<Pena-maan Kode Risiko>	*<Identifikasi risiko aset kritis>*	*<Penyebab risiko terhadap penggunaan aset kritis>*	*<Tindakan yang harus dilakukan untuk mencegah terjadinya risiko>*	*<Berisiko kontrol yang dapat dilakukan berdasarkan panduan untuk melakukan kontrol risiko>*	*<Pihak yang bertanggung jawab atas terjadinya risiko>*

2. Verifikasi Hasil Formulasi Kerangka FMEA yang Disesuaikan

Verifikasi hasil formulasi kerangka FMEA yang Disesuaikan pada Bank XYZ bertujuan untuk melakukan konfirmasi pada perusahaan atas hasil pembuatan kerangka ini berdasarkan hasil penelitian yang telah sesuai dengan kondisi pada Bank XYZ.

Tabel 5.7.5.2. Verifikasi Hasil Formulasi Kerangka FMEA yang Disesuaikan (Sumber: Peneliti, 2014)

FASE	SUB-FASE	ACUAN	STATUS
***Preparation* (Persiapan)**	Memahami Prosedur	***Understanding and Applying the Fundamentals of FMEA*** (Carlson, 2014)	***TERVERIFIKASI***
	Menerapkan Pembelajaran pada Dokumen Audit	***Understanding and Applying the Fundamentals of FMEA*** (Carlson, 2014)	***TERVERIFIKASI***

	Menentukan Penyeragaman Metode Penilaian	***Understanding and Applying the Fundamentals of FMEA*** (Carlson, 2014)	***TERVERIFIKASI***
	Menentukan Pihak yang Berpartisipasi	***Understanding and Applying the Fundamentals of FMEA*** (Carlson, 2014)	***TERVERIFIKASI***
Risk Analyze **(Analisis Risiko)**	Mengidentifikasi Aset Kritis	***FMEA - ASQ Automotive Division Webinar*** (Morris, 2011)	***TERVERIFIKASI***
	Brainstorm Potensi Kegagalan	***FMEA - ASQ Automotive Division Webinar*** (Morris, 2011)	***TERVERIFIKASI***
Risk Scoring **(Penilaian Risiko)**	Menilai Dampak Risiko	***FMEA in Banking*** (Gundry, 2014)	***TERVERIFIKASI***
	Menilai Frekuensi Kemungkinan Risiko	***FMEA in Banking*** (Gundry, 2014)	***TERVERIFIKASI***
	Menilai Deteksi Risiko	***FMEA in Banking*** (Gundry, 2014)	***TERVERIFIKASI***
Risk Priority **(Prioritas Risiko)**	Menghitung Risk Priority Number (RPN)	***FMEA in Banking*** (Gundry, 2014)	***TERVERIFIKASI***
Check and Action **(Cek dan Lakukan)**	Membuat Rekomendasi Kontrol	***FMEA - ASQ Automotive Division Webinar*** (Morris, 2011)	***TERVERIFIKASI***
	Verifikasi Hasil	***FMEA - ASQ Automotive Division Webinar*** (Morris, 2011)	***TERVERIFIKASI***

BAB VI
PENUTUP

Bab ini akan menjelaskan kesimpulan dari penelitian ini, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

6.1. Kesimpulan

Kesimpulan dari penelitian ini adalah sebagai berikut.

Kesimpulan Pertama

Penelitian ini telah menjawab ketiga rumusan masalah penelitian dan tujuan penelitian yaitu:

1. Menghasilkan identifikasi risiko teknologi informasi pada teller Bank XYZ berupa penilaian risiko pada setiap kategori *severity*, *occurence*, dan *detection* yang menghasilkan pemrioritasan risiko berdasarkan kategori RPN.
2. Menghasilkan penilaian risiko teknologi informasi pada teller Bank XYZ yang dilakukan oleh tim A dan tim B, yaitu tidak konsisten. Hasil penilaian risiko menunjukkan RPN berkategori *Very High* sebesar 240, sedangkan tim B hasi RPN pada kategori *Very High* sebesar 567.
3. Menghasilkan Kerangka FMEA yang Disesuaikan yang bertujuan memberikan hasil penilaian menggunakan metode FMEA yang konsisten.

Kesimpulan Kedua

Setiap kesempatan memiliki risiko, hidup tanpa risiko merupakan hidup tanpa kesempatan, dan sering kali hidup tanpa kualitas dan tanpa perubahan.

Sehingga manajemen risiko adalah cara yang tepat untuk melakukan perbaikan kualitas dan melakukan perubahan menjadi lebih baik.

Prosedur yang jelas dalam melakukan penilaian risiko sangat diperlukan sebagai panduan dalam melakukan manajemen risiko untuk mengurangi kemungkinan hasil risiko yang tidak konsisten. Temuan yang didapatkan untuk menghindari kemungkinan hasil yang tidak konsisten adalah, membuat prosedur penilaian risiko, menggunakan suatu metode yang sama, pengetahuan narasumber, kemampuan fasilitator menyampaikan penggunaan kerangka penilaian risiko dalam penelitian ini penggunaan metode FMEA.

6.2. Saran

Saran dari penelitian ini berupa perbaikan untuk keberlanjutan penelitian ini, maupun penelitian selanjutnya. Berikut ini saran yang disampaikan dari penelitian ini.

Saran untuk keberlanjutan penelitian ini

Penelitian mengenai hasil konsisten penggunaan FMEA dan membuat kerangka FMEA yang disesuaikan dengan kebutuhan perusahaan Bank XYZ, dapat dilakukan analisis efektivitas dari penggunaan kerangka FMEA yang Disesuaikan yang telah dibuat oleh peneliti dan membuat evaluasi dari penggunaan kerangka FMEA yang Disesuaikan.

DAFTAR PUSTAKA

Arunachalam, V., & Jegadheesan, C. (2006). Modified Failure Mode and effects Analysis: A Reliability and Cost-based Approach. *The ICFAI Journal of Operations Management*, 7-20.

Bowles, J. B., & Pelaez, C. (1995). Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis. *Journal of Reliability Engineering and System Safety*, 203-213.

Carlson, C. S. (2014). *Understanding and Applying the Fundamentals of FMEA*. Tucson, Arizona USA: ReliaSoft Corporation.

Chen, J. (2007). Utility Priority Number Evaluation for FMEA. *Journal of Failure Analysis and Prevention*, 321 – 328.

Christopher J. Alberts, S. B. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework.* Software Engineering Institute.

Creswell, J. W. (1994). *Research Design: Qualitative and Quantitative Approach.* California: Sage Publication.

Devadasan, S., Muthu, R., Samson, & R.A., S. (2003). Design of total failure mode and effects analysis programme. *International Journal of Quality and Reliability*, 551-568.

DOH. (2007). Independence Choice and Risk: A Guide to Best Practice in Supported Decision Making. London: Department of Health.

Franceschini, F., & Galetto, M. (2001). A New Approach for Evaluation of Risk Priorities of Failure Modes in FMEA. *International Journal of Production Research*, 2991-3002.

Gaspersz, V. (n.d.). *All in One Bundle of ISO*.

Goverment, Q. (2014, May). *Business and Industry Portal*. Retrieved from Business Queensland Goverment: https://www.business.qld.gov.au/business/running/risk-

management/information-technology-risk-management/information-technology-risk

Gundry, E. (2014). *Failure Mode and Effects Analysis in Banking.* FIS Consulting Services.

Institute, P. Q. (2008). *Failure Modes and Effects Analysis Guide.*

J. Allen, M. N. (2008). 'Person Centred Risk Course Book. Stockport: HSA Press.

Janneti, A. J. (2012). A representation: Incorporating a needs assessment and gap analysis into the educational design.

Lindlof, T. R. (2002). *Qualitative Communication Research Methods.* Sage Publication.

M.T. Oldenhofa, J. v.-R. (2011). Consistency of FMEA used in the validation of analytical procedures. *Journal of Pharmaceutical and Biomedical Analysis*.

M.T. Oldenhofa, J. v.-R. (2011). Consistency of FMEA used in the validation of analytical procedures. *Journal of Pharmaceutical and Biomedical Analysis*, 592-595.

Mccuaig, B. (2008). *Fundamentals of GRC: Mastering Risk Assessment.* Thomson Reuters.

McCuaig, B. (2008). Fundamentals of GRC: Mastering Risk Assessment.

Michael Versace, M. A.-M. (2013, November). Retrieved January 2015, from International Data Corporation: http://www.idc.com/getdoc.jsp?containerId=FI244586

Moleong, L. J. (2007). *Metodologi Penelitian Kualitatif.* Bandung: PT Remaja Rosdakarya.

Morris, M. A. (2011). *Failure Mode and Effects Analysis based on FMEA 4th Edition.* M and M Consulting.

Narayanagounder, S., & Gurusami, K. (2009). A New Approach for Prioritization of Failure Modes in Design FMEA Using ANOVA. *World Acedemy of Science Engineering Technology*, 524-531.

Neuman, W. L. (1997). *Sosial Research Methods: Qualitative and Quantitative Approaches.* Allyn and Bacon: Needham Heights.

NewZealandStandards. (1999). *Risk Management Standards and Handbooks*. Retrieved from The New Zealand Society for Risk Management: http://www.risksociety.org.nz/Standards_and_handbooks

Rhee, S., & Ishii, K. (2003). Using Cost based FMEA to Enhance Reliability and Serviceability. *Journal of Advanced Engineering Informatics*, 179-188.

Robillard, L. (2011, August 27). *Integrated Risk Management Framework*. Retrieved Desember 12, 2014, from Treasury Board of Canada Secretariat: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12254&section=text

Silberman, P. B. (2008). *Modelling Risk Management in Inclusive Settings.* London: National Development Team.

Stamatis, D. H. (1995). *Failure Mode and Effect Analysis: FMEA from Theory to Executoion.* New Yourk: ASQC Press.

Sutrisno, A., & Lee, T.-R. (2011). *Service Realiability Assessment Using Failure Mode and Effect and Analysis (FMEA): Survey and Opportunity Roadmap.* International Journal of Engineering, Science, and Technology.

Teng, S. H., & Ho, S. (1996). Failure mode and effects analysis-An integrated approach for product design and process control. *nternational Journal of Quality and Reliability*, 8-26.

Villacourt, M. (1992). Failure Mode and Effect Analysis (FMEA) : A Guide for Continous Improvement for the Semiconductor Equipment Industry, Technology Transfer. *Sematech*.

Yeh, R. H., & Hsieh, M. (2007). Fuzzy Assessment of FMEA for Sewage Plant. *Journal of the Cinese Institute of Industrial Engineers*, 505-512.

LAMPIRAN

Lampiran yang berisikan dokumen pendukung yang dilakukan pada penelitian pada Formulasi Kerangka FMEA yang Disesuaikan yang terdiri dari dokumen prosedur dalam melakukan analisis risiko menggunakan metode FMEA dan hasil wawancara yang dilakukan untuk menggali informasi mengenai kondisi perusahaan.

KODE LAMPIRAN	LAMPIRAN
A	Lampiran Prosedur Riview Dokumen Audit
B	Lampiran Prosedur Penggunaan Skala Penilaian Risiko Metode FMEA
C	Lampiran Prosedur Penetapan Tim Risiko
D	Dokumentasi Wawancara Analisis Risiko
E	Biografi Penulis

BIOGRAFI PENULIS

Penulis, Brigitta Devianti Cahyabuana, lahir di Surabaya, 8 Maret 1993 memiliki hobi berwisata dan mengabadikan momen disetiap perjalanannya. Seperti kutipan salah satu tokoh terkenal, Walt Disney, "*If You Can Dream It, You Can Do It*" dijadikan kutipan semangat dalam mewujudkan mimpi-mimpinya.

Pendidikan formal yang telah dienyam oleh penulis di SMP Negeri 12 Surabaya, SMA Negeri 6 Surabaya, hingga meneruskan pendidikan dan mendapat gelar sarjana di Jurusan Sistem Informasi, Institut Teknologi Sepuluh Nopember.

Prestasi yang pernah diraih oleh penulis mendapatkan pendanaan pada Program Kreativitas Mahasiswa (PKM) 2012 kategori Kewirausahaan, dilanjutkan dengan mengikuti program *ASEAN Youth Leaders Exchange* (AYLE) di Fillipina pada tahun 2013 yang diadakan oleh National University of Singapore. Dan bekesempatan mendapatkan beasiswa untuk mengembangkan usaha dibidang industri kreatif melalui Beasiswa Teknologi Industri Kreatif (BUTIK) 2013 yang diadakan oleh CIMB Niaga dan Kementrian Pendidikan dan Kebudayaan Republik Indonesia (Kemdikbud RI)

Penulis dapat dihubungi melalui email jika ada pertanyaan, saran, dan kritik untuk menjadi bahan diskusi, brigitta.cahyabuana@gmail.com.