Analisis, Evaluasidan Mitigasi Risiko Aset Teknologi Informasi Menggunakan*Framework* OCTAVE dan FMEA Pada Bank Jateng Cabang Jepara

Pristyanti Nawang Putri[1], Heru Pramono Hadi[2]
[1,2] Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
Jl. Nakula I, No.1-11, Semarang, Kode Pos 50131, Telp. (024)3515261 Fax :3569684
e-mail: [1]**pristyantinawangp@gmail.com**, [2]**heru.pramono.hadi@dsn.dinus.ac.id**

Abstrak

Penerapan teknologi informasi pada sektor perbankan dapat membantu proses pengelolaan dan pengolahan informasi yang telah dilakukan oleh Bank Jateng Cabang Jepara, seperti kegiatan pengelolaan data dan informasi yang proses aktivitasnya berkaitan langsung dengan nasabahnya. Permasalahan yang sering dialami kehilangan data yang disebabkan oleh virus, data rusak, pengulangan data, maupun hak akses yang disalahgunakan oleh pihak terkait. Kejadian tersebut mengakibatkan semua kegiatan operasional terganggu dan terhenti. Tujuan dari penelitian ini adalah untuk mengetahui apa saja aset TI yang ada di perusahaan, menganalisis dan mengevaluasi dalam memperkecil risiko yang terjadi pada setiap aset TI sertamengetahui hasil penilaian atas mitigasi risiko aset teknologi informasi. Metode penelitian yang digunakan adalah Octave untuk mengelola risiko aset TI dan FMEA untuk melakukan penilaian terhadap masing-masing risiko, yang kemudian diberikan ranking berdasarkan prioritasnya. Hasil yang diperoleh dari penelitian ini adalah ranking yang mempunyai 7 risiko level *very high*, 11 risiko level *high*, 12 risiko level *moderate*, 21 risiko level *low*, 3 risiko level *very low*. Sehingga dari hasil RPN, yang perlu diberikan penangan khusus yaitu RPN yang mempunyai level *very high* dan *high.* Serta dengan menerapkan kontrol ISO 27002:2013 sebagai pengendalian dan prosedur Sistem Manajemen Keamanan Informasi untuk meminimalisir atau mengilangkan suatu risiko.

Kata kunci*— Mitigasi Risiko, Teknologi Informasi, Aset, OCTAVE, FMEA, ISO 27002:2013.*

Abstract

Implementation of information technology in the banking sector can assist the process of managing and processing information that has been done by Bank Jateng Jepara Branch, such as data and information management activities that process activities directly related to its customers. Problems often experienced data loss caused by viruses, corrupted data, repetition of data, or access rights that are misused by related parties. The incident resulted in all operational activities disrupted and stopped. The purpose of this study is to find out what are the existing IT assets in the company, analyze and evaluate in minimizing the risk that occurs on each IT asset and know the results of the assessment of risk mitigation of information technology assets. The research method used is Octave to manage the risk of IT assets and FMEA to assess each risk, which is then ranked by priority. The results obtained from this research are rank that has 7 very high level risk, 11 high risk level, 12 moderate risk level, 21 low risk level, 3 very low risk level. So from the results of RPN, which needs to be given a special handler that is RPN that have very high level and high. And by applying ISO 27002: 2013 control as a control and procedures Information Security Management System to minimize or eliminate a risk.

Keywords—*Risk Mitigation, Information Technology, Assets, OCTAVE, FMEA, ISO 27002: 2013*

1. PENDAHULUAN

Teknologi informasi adalah faktor pendukung dari berjalannya suatu proses bisnis dari suatu organisasi pada era globalisasi yang semakin berkembang pesat. Penerapan teknologi informasi memerlukan faktor pendukung yang memadai sehingga dalam menjalankan bisnis tersebut bisa mendapatkan tujuan yang diharapkan. Mengenai dengan penyedia layanan perbankan yang menginginkan informasi sebagai wadah keberhasilan atas kinerjanya. Penerapan teknologi informasi pada sektor perbankan dapat membantu proses pengelolaan dan pengolahan informasi yang telah dilakukan oleh Bank Jateng Cabang Jepara, seperti kegiatan pengelolaan data dan informasi yang proses aktivitasnya berkaitan langsung dengan nasabahnya. Namun dengan segala kemungkinan yang telah didapatkan, tidak dapat dipungkiri bahwa dalam memanfaatkan teknologi informasi mempunyai berbagai risiko yang beragam.

Dalam pelaksanaan mitigasi risiko diperlukan kerjasama dari berbagai pihak terkait untuk menyusun prosedur dan penerapan kebijakan dari risiko teknologi informasi. Dengan menerapkan metode yang sama dengan kondisi yang dibutuhkan perusahaan untuk menyelesaikan masalah menjadi lebih cepat dan tepat.

Penggunaan metode *Operationally Critical Trait, Asset and Vunerabillity Evaluation* (OCTAVE) merupakan suatu strategi dan perencanaan implementasi guna keamanan informasi atas risiko, dan pemakakaian prosedur FMEA (*Faillure Mode And Effect Analysis*) Metode FMEA merupakan penilaian risiko IT untuk memberitahu informasi mengenai kendala risiko, desain, dan proses. Penerapan kontrol ISO yang digunakan yaitu ISO 27002:2013 yaitu berisi tentang panduan untuk menangai risiko yang digunakan tersebut sebagai saran tindakan untuk perbaikan. [3]

2. METODE PENELITIAN

2.1 Metode Pengumpulan Data

1. Wawancara

Wawancara merupakan metode pengumpulan data secara langsung kepada pihak yang bersangkutan dalam bentuk tanya jawab. Dalam penelitian ini dilakukan untuk mendapatkan informasi yang berkaitan dengan proses identifikasi aset kritis serta masalah apa saja yang sering terjadi, yaitu dengan cara berinteraksi langsung dengan pegawai bagian IT Bank Jateng Cabang Jepara.

2. Studi Literatur

Studi Literatur merupakan metode pengumpulan data untuk mendukung kajian penelitian yang dilakukan penulis untuk mencari dan mengumpulkan beberapa sumber data yang diperoleh dari buku, jurnal, e-book, catatan atau dokumen dan situs online yang masih ada kaitannya dengan penelitian ini, diantaranya mengenai sistem informasi, mitigasi risiko, OCTAVE, FMEA.

2.2 Jenis Data

1. Data Kualitatif

Data Kualitatif merupakan sumber data informasi terhadap suatu masalah dari objek yang diteliti. Dalam kegiatan ini informasi-informasi yang didapat bisa melalui analisis dokumen, observasi, wawancara, ataupun diskusi dengan salah satu pegawai Bagian IT pada Bank Jateng Cabang Jepara. Dan dalam penelitian ini data kualitatif mengacu pada penggunaan metode

octave. Karena metode octave sesuai digunakan untuk menganalisis aset-aset TI pada organisasi/perusahaan.

2. Data Kuantitatif

Data Kuantitatif merupakan sumber data informasi terhadap suatu masalah yang bisa diperoleh secara sistematis dan ditentukann dengan angka tertentu.Dalam kegiatan ini informasi-informasi atau data-data yang didapat yaitu mengacu pada penggunaan metode fmea. Karena metode fmea sesuai digunakan untuk menentukan penilaian atas risiko aset yang menghasilkan nilai RPN.

2.3 Sumber Data

1. Data Premier

Data primer merupakan sumber data yang diperoleh dari data asli tanpa ada perubahan apapun oleh pihak terkait. Dalam kegiatan ini data premier berupa wawancara dan observasi. Data premier penelitian ini diperoleh langsung dari pegawai Bagian IT pada Bank Jateng Cabang Jepara.

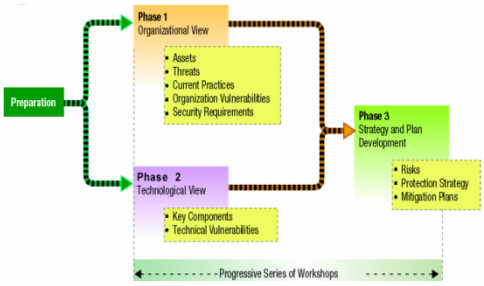
2. Data Sekunder

Data sekunder merupakan sumber data yang diperoleh tidak melalui pihak terkait sacara langsung namun melalui pihak kedua sumber-sumber lain. Dalam kegiatan ini berupa referensi buku, data laporan dan jurnal yang berkaitan dengan manajemen risiko dan keamanan aset TI.

2.4 Metode Analisis

1. Metode OCTAVE

Metode OCTAVE yang digunakan untuk mengolah data dari hasil wawancara. Dalam kegiatan ini, metode OCTAVE yang digunakan untuk mengidentifikasi risiko berdasarkan data yang sudah diperoleh. [2]



Gambar 1. Fase Metode OCTAVE [2]

Fase Pertama: Membangun profil ancaman dan berdasarkan aset pada organisasi.
Merupakan aspek evaluasi atas organisasi. Tim analisis dari organisasi berkontribusi tentang apa yang penting bagi organisasi dan apa yang saat ini sedang dilakukan untuk melindungi aset-aset tersebut

Fase kedua: Identifikasi kerentanan infrastruktur.
Merupakan aspek pengembangan atas infrastruktur komputasi. Tim analisis mengidentifikasi sistem teknologi informasi kunci dan komponen yang terkait pada setiap aset kritis.

Fase ketiga: Membangun strategi keamanan dan rencana organisasi.
Bagian dari proses evaluasi, tim analisis mengidentifikasi proses untuk dianalisa risiko yang membahayakan dalam organisasi dan mengambiil langkah yang tepat untuk penyelesaian kemudian menyusun rencana untuk mengatasi risiko tersebut berdasarkan hasil analisa-analisa yang telah terkumpulkan.

2. Metode FMEA

Metode FMEA digunakan untuk memberikan nilai/rate yang sudah teridentifikasi oleh metode octave. Metode ini juga digunakan untuk pemberian bobot atas peluang terjadinya kegagalan dalam sistem, proses, serta produk maupun servis untuk menentukan tingkat keseriusan efek yang ditimbulkan.[3]

Tahapan penilaian FMEA:

1. Severity (S): Tingkat keparahan, merupakan penilaian seberapa serius efek atas kegagalan yang berpotensial terjadi dari skala 1-10 dimana 1 adalah paling rendah. 2. Occurence (O): Keterjadian, seberapa sering terjadinya kegagalan pada suatu aset dari skala 1-10 dimana 1 adalah paling rendah.
3. Detection (D): Merupakan penilaian atas kemungkinan terdeteksinya penyebab terjadinya suatu bentuk kegagalan pada aset dari skala 1-10 dimana 1 adalah paling tinggi.
4. Risk Priority Number (RPN): Merupakan hasil prioritas risiko yang didapat dari pengalian Severity, Occurence dan Detection dengan rumus RPN= S x O x D.

Tabel 1. Nilai RPN [5]

Level	Nilai RPN
Very Low (Sangat Rendah)	0 sampai 20
Low (Rendah)	21 sampai 70
Moderate (Sedang)	71 sampai 110
High (Tinggi)	111 sampai 199
Very High (Sangat Tinggi)	Lebih dari 200

3. HASIL DAN PEMBAHASAN

3.1 Mengidentifikasi Aset Kritis

Daftar Aset Kritis pada Bank Jateng Cabang Jepara yang didapat dari Pegawai Bagian IT yaitu sebagai berikut:[4]

Tabel 2. Mengidentifikasi Aset Kritis

Kelompok Aset	Aset Kritis	Penjelasan
Hardware	Komputer (CPU, Monitor)	Digunakan untuk membantu proses bisnis utama pada Bank.
	Router	Digunakan untuk menghubungkan antar jaringan yang sama ataupun berbeda yang dapat digunakan untuk mengirimkan data dari jaringan yang satu ke yang lainnya.
	Printer	Perangkat keras yang digunakan untuk mencetak suatu dokumen.
	Switch	Alat yang dapat digunakan untuk mengubungkanjaringan

Kelompok Aset	Aset Kritis	Penjelasan
		dengankomputer.
	Server	Digunakan sebagai bentuk data*storage* dan dapat memberikan layanan atas komputer *client*.
	Kabel jaringan	Kabel yang digunakan untuk menghubungkan jaringan dengan Komputer/Server /Switch/Router.
	CCTV	Digunakan untuk merekam semuakondisi.
	OS/*Operating System* (Windows)	*Operating system* yang digunakan pada komputeruntuk menjalankan program-program/kegiatan dalam pelaksanaan proses bisnis.
	IBM/Green Screen	*Software* aplikasi yang digunakan untuk mengakses data ke core/data center.
	Web Branch	*Software* aplikasi yang digunakan harian untuk transaksi dari monitoring, kredit, dan transaksi-transaksi lainnya, tetapi hanya saja webbranch sudah GUI
Software	SIM SDM	*Software* aplikasi yang digunakan untuk aplikasi SDM (Sumber Daya Manusia), untuk membuat data pegawai, mutasi/ pengurangan pegawai, daftar gaji/upah, cuti pegawai, dan lainnya
	Business Intelligence	*Software* aplikasi yang digunakan untuk mendapatkan informasi-informasi lengkap tentang perkembangannya bank, laporan operasional, dll
	Aplikasi (Ms. Office)	*SoftwareAplication* pendukung yang digunakan untuk memproses kegiatan yang ada dikantor/organisasi.
	Antivirus (Simantex & Point Protection)	*Software* yang gunanya untuk melindungi komputer dari serangan virus, *malware* maupun *spyware*.
Network	Jaringan internet	Proses bisnis kantor dilakukan dengan bantuan internet karena sebagian data diakses melalui internet secara online.
	Jaringan Intranet	Penggunaan intranet dapat

Kelompok Aset	Aset Kritis	Penjelasan
		mengkomunikasikan komputer satu dengan yang lain, seperti internet tatapi layanannya terbatas, tidak seluas dan seberagam di internet.
Pengguna/*People*	Admin	Sumber Daya Manusia yang melaksanakan proses bisnis.
Data	Data Pegawai	Berisikan data yang terkait pegawai Bank Jateng Cabang Jepara
	Data User Pegawai	Berisikan data*userid* yang terkait pegawai Bank Jateng Cabang Jepara.
	Data Workstation	Berisikan data terkait *ip* pegawai Bank Jateng Cabang Jepara.
	Data Printer (Print Server)	Berisikan data terkait nomor printer tiap divisi Bank Jateng Cabang Jepara.
	Elektronik Jurnal ATM	Berisikan history transaksi ATM dari salinan/*copy*-an cetakan stuck sampai capture image, dan dilanjutkan dengan masukkan kartu ATM sampai take cash/ambil uang
	Transaksi COA/General Ledger	Berisikan mutasi keluar masuk pendapatan biaya dan tambah kurangnya aktiva pasiva

3.2 Keperluan Keamanan

Setelah melakukan wawancara, didapatkan informasi mengenai aset kritis pada perusahaan, kemudian menentukan berdasarkan keperluan keamanan informasi terhadap aspek *Confidentiality, Integrity, Availability* (CIA) yang terdiri atas:[6]

1. *Confidentiality* (Kerahasiaan) merupakan salah satu aspek penting dalam menjaga keamananinformasi hanya bisa diakses oleh orang yang memiliki wewenang dan menjamin kerahasiaan informasi. Segala upaya atau cara agar tersimpannyatidak tersebarnya suatu informasi dari bahaya/risiko penyalahgunaan.
2. *Integrity* (Integritas) merupakan semua informasi yang tersedia yang ditujukan pada pihak-pihak yang memerlukan data yang akurat tanpa ada perubahan ataupun kebohongan data.
3. *Availability* (Ketersediaan) merupakan informasi data-data yang ada juga harus ditunjukan ke pihak-pihak yang berkepentingan dalam mengolah atau memperoleh informasi oleh karenanya diperlukan ketersediaan informasi untuk mengaksesnya tanpa ada gangguan apapun.

3.3 Ancaman Pada Aset Kritis

Ancaman aset kritis ditentukan berdasarkan kemungkinan terjadi atas aset, ancaman ditentukan dengan melakukan brainstorming dengan Pegawai Bagian IT.[1]

3.4 Melakukan Penerapan Keamanan

1. Melakukan pelatihan dasar pada aset yang dimiliki dan pihak terkait divisi TI harus memahaminya. Mengenai dengan perihal ini dalam penggunaan aset yang ada harus sesuai dengan proses/tata cara yang semestinya.
2. Memberikan pembatasan pada hak akses. Setiap admin yang ada mempunyai kewenangannya sendiri, yaitu dengan memiliki password dan username untuk setiap staff agar perubahan data yang ada dapat dilakukan oleh setiap admin staff terkait.
3. Penggunaan aplikasi mempunyai lisensi resmi. Adanya lisensi resmi/asli diharapkan untuk memperkecil atau meminimalisir resiko pada saat kegagalan terjadiketika digunakan.
4. Melaksankan *Back-up* data. Pada pihak ketiga telah melakukan backup data yang dalam kasus ini yaitu kantor pusat, tetapi pada pihak Kantor Bank Jateng Cabang Jepara harus tetap melakukan back-up data secara rutin agar tidak ada data yang rusak dan hilang atau terjadi sesuatu atas penyimpanan utamanya.

3.5 Kelemahan Pada Bagian IT

1. Kurangnya dalam Sumber Daya Manusia (SDM) yang berkompeten.
2. Kurangnya jumlah CCTV, sehingga tidak dapat mengawasi/merekam kondisi pada ruangan bagian TI secara jelas.
3. Dalam memperbarui workstation harus dilakukan ke kantor pusat dulu.
4. Belum adanya fasilitas untuk me-*reset* password user id, jadi harus dilakukan oleh kantor pusat.

3.6 Mengidentifikasi Komponen Kunci *(Key Component)*

Komponen kunci merupakan komponen yang mempunyai tujuan atau digunakan untuk melaksanakan proses bisnis utamanya. Berikut ini merupakan komponen kunci di Bank Jateng Cabang Jepara:

Tabel 3. Mengidentifikasi Komponen Kunci

Jenis	Komponen Kunci	Keterangan
Hardware	Komputer (CPU, Monitor)	Digunakan untuk membantu proses bisnis utama pada Bank.
	Server	Digunakan sebagai bentuk *storage*data dan dapat memberikan layanan atas komputer *client*.
	Printer	Perangkat keras yang digunakan untuk mencetak suatu dokumen.
Software	OS/*Operating System*(Windows)	*Operating system* yang digunakan pada komputeruntuk mengoperasikan program-program/ kegiatan dalam melaksanakan proses bisnis.
	Aplikasi (*MS.office*, IBM/Green Screen, Web Branch, SDM SIM, Business Intelligence)	*Software* aplikasi pendukung yang dipakaiuntuk memproses kegiatan yang ada dikantor/organisasi.
Network	Jaringan Internet dan Intranet	Proses bisnis kantor dilakukan dengan bantuan internet karena sebagian data diakses melalui internet secara online.

Jenis	Komponen Kunci	Keterangan
Pengguna/*People*	Pegawai/Karyawan	Admin yang melakukan/ menjalankan proses bisnis pada bagian TI.
Data	*Database*	*Storage* data yang saling berhubungan dengan proses bisnis yang dilakukan oleh bagianTI.

3.7 Evaluasi Komponen Kunci

Komponen Kunci dievaluasi untuk menentukan kemungkinan kelemahan dan penjelasannya.

3.8 Menganalisis Atas Risiko Aset Kritis

Pada bagian ini akan dilakukan analisis risiko agar dapat mengetahui risiko dengan menentukan dampak serta penyebab dari risiko atas aset kritis TI.

3.9 Penilaian Atas Risiko Aset

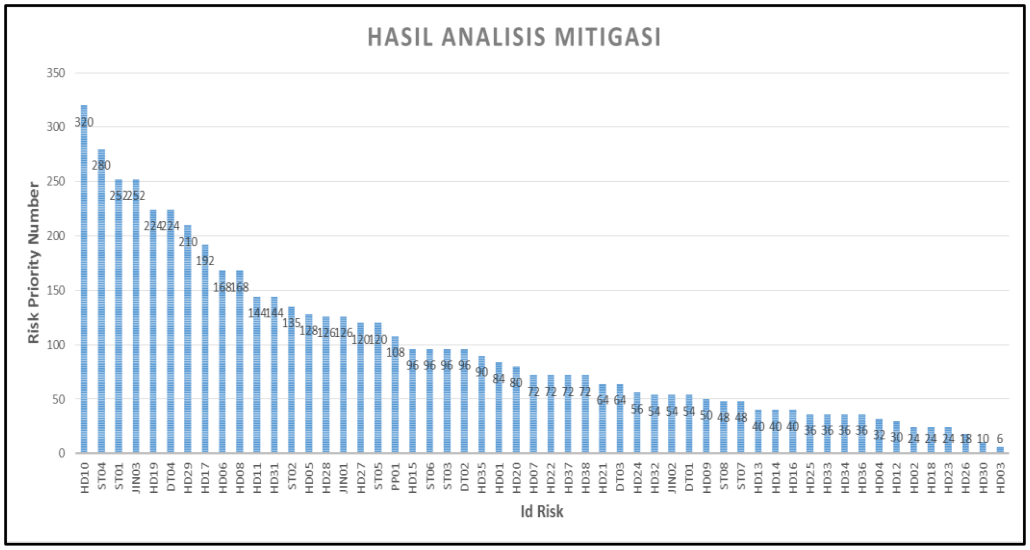
Setelah melakukan analisis risiko atas aset kritis kemudian risiko tersebut diberikan penilaian untuk dapat mengetahui tingkat keseriusan risiko dengan memanfaatkan metode FMEA. Dengan memanfaatkan metode tersebut akan menghasilkan tingkat keseriusan pada risiko.

3.10 Penilaian Kedudukan Atas Risiko Aset

Perankingan risiko dilakukan dengan mengurutkan jumlah RPN tiap aset dari tertinggi hingga terendah.

3.11 Grafik Hasil Analisis Mitigasi Risiko

Pengelompokan penilaian kedudukan atas risiko aset IT pada Bank Jateng Cabang Jepara agar memudakan untuk pembuatan grafik selanjutnya:



Gambar 4. Hasil Analisis Mitigasi Risiko

3.12 Mitigasi Risiko

Mitigasi risiko ditentukan tindakan yang disarankan yang sama dengan tipenya. Ada empat (4) tipe mitigasi risiko tersebut diantaranya *Transference, Limitation, Acceptance Avoid:*

1. Risk Acceptence
   Risiko nantinya tetap diterima namun teknologi informasi tetap dijalankan untuk menerapkan kontrol dan nantinya risiko akan diturunkan ke tingkat yang lebih rendah
2. Risk Limitation
   Membatasi risiko dengan melakukan kontroling agar dampaknya dapat diminimalisir dan tidak menimbulkan kerugian yang besar
3. Risk Transference
   Risiko diserahkan kepada pihak ketiga untuk dilakukan perbaikan karena pihak perusahaan tidak kompeten atau mengganti kerugian.
4. Risk Avoid
   Risiko dihindari dan dihilangkan penyebabnya agar tidak menyebabkan kerugian dan biasanya memerlukan biaya yang besar

3.13 Penggunaan Kontrol ISO 27002:2013

ISO 27002:2013 membantu dalam penyusunan pedoman untuk penerapan standar control kemanan informasi pada tiap-tiap pemicu risiko atas asset IT pada Bank Jateng Cabang Jepara. Dibawah ini merupakan *Objective Control* atas risiko dengn level *very high* serta *high.*[7]

Tabel 5. Kontrol ISO 27002:2013

ID Risk	***Potensial Cause***	***ControlObjective***
		A.7.2.1 *Management responsibilities*(tanggung jawab management)
		Management bertanggungjawab atas karyawan dalam menjaga keamanan informasi sesuai dengan persyaratan padaketetapan serta mekanismeatas perusahaan, untuk itu diharapkan karyawan tidak asal-asalan dalam melakukan penggunaanpada media *eksternal storage.*
		A.8.3.1 *Management of removable media*(pengelolaan media pemindahan)
HD10	Terserang virus dari media penyimpanan *eksternal* ataupun yang didapat pada saat beroperasi di internet.	Mekanisme yang ada harus jelas dengan itu dapat dilakukan penerapanpada pengelolaan media *eksternal storage.*
		A.11.2.8 *Unattended user equipment*(peralatan pengguna tanpa ada pengawasan)
		*User*harus mempunyai keyakinanmaka pemakaiaan media *eksternal* yang belum tercatat mempunyai cukup *proteksi.*
		A.12.2.1 *Controls against malware*(kontrol teradap malware)
		Harus diterapkannya pendeteksian kontrol, pencegahan serta perbaikan akibat malware, dan perlu juga disertai dengan sikap hati-hati/kewaspadaan dari pengguna.
ST04	Aplikasi yang tidak asli untuk itu	A.12.5 *Control of operational software*

ID Risk	*Potensial Cause*	*ControlObjective*
	dapat memberikan efek program error karena penggunaan yang cukup banyak	A.12.5.1 *Installation of software on operational systems*(Pemasangan perangkat lunak pada sistem operasional)
		Prosedur/mekanisme yang jelas diharuskan untuk diimplementasikan dalam mengcontrol pada *processinstallationsoftware*yang terdapat di *operating system.*
		A.7.2.1 *Management responsibilities*(tanggung jawab management)
		Management bertanggungjawab atas karyawan dalam menjaga keamanan informasi sesuai dengan persyaratan padaketetapan serta mekanismeatas perusahaan, untuk itu diharapkan karyawan tidak asal-asalan dalam melakukan penggunaanpada media *eksternal storage.*
		A.8.3.1 *Management of removable media*(pengelolaan media pemindahan)
ST01	Akibat dari penggunaan media *eksternalstorage*yang asal-asalan sehingga rentan virus yang masuk	Mekanisme yang ada harus jelas dengan itu dapat dilakukan penerapanpada pengelolaan media *eksternal storage.*
		A.11.2.8 *Unattended user equipment*(peralatan pengguna tanpa pengawasan)
		*User*harus mempunyai keyakinanmaka pemakaiaan media *eksternal* yang belum tercatat mempunyai cukup *proteksi*.
		A.12.2.1 *Controls against malware*(kontrol teradap malware)
		Harus diterapkannya pendeteksian kontrol, pencegahan serta perbaikan akibat malware, dan perlu juga disertai dengan sikap hati-hati atau kewaspadaan dari pengguna.
		A.13.1.2 *Security of networks services*(Keamanan layanan jaringan)
JIN03	Menurunnya jaringan dari pusat yang menyediakanfasilitas/layanan.	Management diharuskan untuk mengidentifikasi dan memasukkan prosedur keamanan, tahapan servicesertapersyaratan yang dilakukan management dari semua service jaringan tersebut dilakukan kesepakatan kontrak service jaringan, baik itu untuk internal ataupun*network* yang disediakan oleh pihak-pihak lainnya.
		A.11.2.4 *Equipment maintenance*(Pemeliharaan peralatan)
HD19	Akibat dari kurangnya pemeliharaan server, sehinggakerusakan diawal tidak dapat terdeteksi.	Pemeliharaan pada perangkat/peralatanharuslahdilakukan dengan teratur serta baik karena untuk dipastikannya perangkat/ peralatan tsb tetap dapat digunakan kapan sajasaat diperlukan dan integritas yang selalu terjaga.
DT04	Kerusakan data yang dikarenakankesalahan padawaktu proses	A.12.2.1 *Controls against malware*(Kontrol terhadap malware)

ID Risk	*Potensial Cause*	*ControlObjective*
	penyimpananataupundikarenakan serangan malware.	Harus diterapkannya pendeteksian kontrol, pencegahan serta perbaikan akibat malware, dan perlu juga disertai dengan sikap hati-hati/kewaspadaan dari pengguna. A.12.5.1 *Installation of software on operational systems*(Pemasangan perangkat lunak pada sistem operasional) Prosedur/mekanisme yang jelas diharuskan untuk diimplementasikan dalam mengontrol pada proses *installationsoftware*yang terdapat di *operating system*.
HD29	Aliranlistrik terputus dengantiba-tiba atau tidak diinginkan ketika pemakaian komputer berlangsung.	A.11.2.2 *Supporting utilities*(Utilitas pendukung) Perangkat/peralatandiharuskan untuk dilindungi dari kegagalan penyedia tenaga listrik, misalnya dengan menggunakan penyedia tenaga listrik cadangan UPS supaya memberikan waktu untuk menyimpan pekerjaan/kegiatanataupun dalam menghidupkan genset.
HD17	Server terlalu tua atau lama maka tidak mumpuni untuk digunakan. Sehingga harus ada masa pemakaiannya	A.11.2.4 *Equipment maintenance*(Pemeliharaan peralatan) Pemeliharaan pada perangkat/peralatan yang haruslahdilakukan dengan teratur serta baik karena untuk dipastikannya perangkat/peralatan tsb tetap dapat digunakan kapan sajasaat diperlukan dan integritas yang selalu terjaga.
HD06	Penggunaankomputer (PC) oleh pengguna tidak sesuai dengan mekanismeyang ada atau tidak dengan semestinya.	A.12.1.1 *Documented operating procedures*(Prosedur/mekanisme operasi terdokumentasi) Mekanisme operasi diharuskan mempunyai dokumentasi serta diharuskan siap sedia saat pengguna yang mempunyai hakdiwaktu membutuhkan.
HD08	Memaksakan susunan/ konfigurasi komputer (PC)yang diharuskan meskipun tidak sesuai.	A.11.2.4 *Equipment maintenance*(Pemeliharaan peralatan) Pemeliharaan pada perangkat/peralatanharuslahdilakukan dengan teratur serta baik karena untuk dipastikannya perangkat/peralatan tsb tetap dapat digunakan kapan sajasaat diperlukan dan integritas yang selalu terjaga.
HD11	Aliran listrik terputus pada saatkomputer (PC) sedang digunakan.	A.11.2.2 *Supporting utilities*(Utilitas pendukung) Perangkat/peralatandiharuskan untuk dilindungi dari kegagalan penyedia tenaga listrik, misalnya dengan menggunakan penyedia tenaga listrik cadangan UPS supaya memberikan waktu untuk menyimpan pekerjaan/kegiatanataupun dalam menghidupkan genset.
HD31	Perangkat mengalami konsleting.	A.11.2.4 *Equipment maintenance*(Pemeliharaan peralatan) Pemeliharaan pada perangkat/peralatanharuslahdilakukan dengan teratur serta baik karena untuk dipastikannya perangkat/ peralatan tersebut tetap dapat digunakan kapan sajasaat diperlukan dan integritas yang selalu terjaga.

ID Risk	*Potensial Cause*	*ControlObjective*
ST02	Gagalnya antivirus pada saatmemulai *scan* virus atau *malware* yang dimiliki	A.12.2.1 *Controls against malware*(Kontrol terhadap malware) Harus diterapkannya pendeteksian kontrol, pencegahan serta perbaikan akibat malware, dan perlu juga disertai dengan sikap hati-hati/kewaspadaan dari pengguna. A.12.5.1 *Installation of software on operational systems* (Pemasangan perangkat lunak pada sistem operasional) Prosedur yang jelas diharuskan untuk diimplementasikan dalam mengontrol pada proses *installationsoftware*yang terdapat di *operating system*.
HD05	Pemeliharaankomputer (PC) tidak teratursehingga pemeliharaanuntuk bagian komputer (PC) yangdibutuhkan telah terabaikan.	A.11.2.4 *Equipment maintenance*(Pemeliharaan peralatan) Pemeliharaan pada perangkat/peralatanharuslahdilakukan dengan teratur serta baik karena untuk dipastikannya perangkat/ peralatan tersebut tetap dapat digunakan kapan sajasaat diperlukan dan integritas yang selalu terjaga.
HD28	Pemakaian server tanpa ada berhentinyaserta pendinginnya tidak dapat beroprasi	A.11.2.4 *Equipment maintenance*(Pemeliharaan peralatan) Pemeliharaan pada perangkat/peralatanharuslahdilakukan dengan teratur serta baik karena untuk dipastikannya perangkat/ peralatan tsb tetap dapat digunakan kapan sajasaat diperlukan dan integritas yang selalu terjaga.
JIN01	Pengamanannya kurangpada jaringan yang dimiliki,untuk itumemungkinkan *hacking*dapat kejadian	A.13.1.1 *Network Controls*(kontrol jaringan) *Network Controls*diharuskan untuk dikelola/dijalankanserta dicontrol untuk melakukan perlindungan asset yang dimiliki dan juga yang berhubungan dengan *network*. A.13.1.2 *Security of networks services*(Keamanan layanan jaringan) Management diharuskan untuk mengidentifikasi dan memasukkan prosedur keamanan, tahapan servicesertapersyaratan yang dilakukan management dari semua service jaringan tersebut dilakukan kesepakatan kontrak service jaringan, baik itu untuk internal ataupun*network* yang disediakan oleh pihak-pihak lainnya.
HD27	Server yang banyak digunakan/diakses pada satu waktu/saat bersamaan.	A.9.3 *Responsbility for user* (tanggungjawab atas pengguna) Pengguna bertanggungjawab atas pemakaian server dalam satu waktu yang bersamaan, sehingga diharapkan pemakaian server digunakan sesuai dengan persyaratan padaketetapan serta mekanismeatas perusahaan, karyawan tidak asal-asalan dalam melakukan

ID Risk	*Potensial Cause*	*ControlObjective*
		penggunaanserver.
ST05	Akibat dari kurangnya pemeliharaan,sehingga kerusakan diawal tidak dapat terdeteksi.	A.11.2.4 *Equipment maintenance*(Pemeliharaan peralatan) Pemeliharaan pada perangkat/peralatanharuslahdilakukan dengan teratur serta baik karena untuk dipastikannya perangkat/ peralatan tsb tetap dapat digunakan kapan sajasaat diperlukan dan integritas yang selalu terjaga.

4. KESIMPULAN

1. Pada saat menentukan penilaian pada aset TI yang dipunyai Bank Jateng Cabang Jepara penelitian ini menggunakan perhitungan Risk Priority Number (RPN) yang diambil dari perkalian faktor yaitu Saverity, Occurance, Detection yang mempunyai nilai dari 1 sampai 10
2. Dari penilaian yang sudah dilakukan/dibuat dengan menggunakan metode *Faillure Mode and Effect* (FMEA), *control action* risiko pada level risko *very high* dan *high.* Perihal ini dilakukan karena risiko dengan ranking *very high* dan *high* memberi pengaruh yang begitu besar/banyak pada suatu perusahaan makadari itu risiko bisa di perkecil ataupun bisa dilakukan pencegahan sebelum terjadi.
3. Dari proses mengidentifikasi risko asset TI yang ada pada Bank Jateng Cabang Jepara diketahui 54 risiko dimana terdapat risiko didalamnya ranking yang diperoleh masing-masing 7 risiko mempunyai level *very high*, 11 risiko mempunyai level *high*, 12 risiko mempunyai level *moderate*, 21 risiko mempunyai *level low*, 3 risiko mempunyai level *very low.*

5. SARAN

1. Divisi TI perlu melakukan pencatatan data mengenai risiko-risiko yang terjadi setiap tahunnya agar dapat digunakan oleh pihak manajemen dalam membuat keputusan dan rencana strategis perusahaan dalam bidang TI
2. Dapat melakukan penerapan dengan metode dan menggunakan standar ISO yang berbeda agar dapat mengerti/memperoleh hasil yang lebih bervariatif serta sesuai dengan keperluan pada Kantor Bank Jateng Cabang Jepara. Sebagai contoh ISO 14001 yang menjelaskan tentang standar dengan ketentuan *environmental management system* yang digunakan pada perusahaan untuk mengidentifikasi atas aspek dan pengaruh lingkungan yang di sebabkan dari kegiatan ataupun operasi organisasi terhadap faktor lingkungan. Untuk itu organisasi lebih dapat melakukan penghematan energy, air, ataupun bahan bakar sehingga membawa keuntungan/ manfaat dalam perihal finansial.

DAFTAR PUSTAKA

[1] "Definisi-Pengertian.Com," 2015. [Online]. Available: http://www.definisi-pengertian.com/2015/05/jenis-jenis-risiko.html. [Diakses 11 Maret 2017].

[2] A. D. Christopher Albert, "Introduced to the OCTAVE Approuch," dalam *PA, Carnegie Mellon*, 2003, pp. 1-37.

[3] Idham Pamungkas, "Failure Modes And Effect Analysis," 23 april 2014. [Online].http://www.academia.edu/7652952/Failure_Modes_and_Effect_Analysis. [Diakses maret 2017].

[4] C. S. Carlson, "Understanding And Applying the Fundamentals of FMEAs," dalam *2014 Annu. Reliab. Maintainab. Symp*, 2014, p. 12.

[5] R. J. M. M. R. B. Robin E. McDermott, "The Basics of FMEA 2nd Edition," dalam *Taylor & Francis Group, LLC Productivity Press is an imprint of Taylor & Francis Group, an Informa business* , New York, NY 10016, 2009, pp. 34-50.

[6] M. A. Azali, "Sistem Terdistribusi 014 - Keamanan," 2015. [Online]. Available: http://slideplayer.info/slide/1915103/. [Diakses maret 2017].

[7] I. 27002, "ISO/IEC 27002 : Information Technology - Security Techniques - Code of practice for infomation security controls," 2016. [Online]. Available: http://www.iso27001security.com/html/27002.html. [Diakses 13 Maret 2017].