PENILAIAN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE *FAILURE MODE AND EFFECTS ANALYSIS* DI DIVISI TI PT. BANK XYZ SURABAYA

Innike Desy[1)], Bekti Cahyo Hidayanto[2)] Hanim Maria Astuti[3)]
[1]Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember
Jl. Raya ITS Kampus ITS Sukolilo, Surabaya, 60111
Telp : (031) 5999944, Fax : (031) 5964965
E-mail : innike09@mhs.is.its.ac.id[1)], bekticahyo@is.its.ac.id[2)], hanim@is.its.ac.id[3)]

Abstrak

Sebagai lembaga keuangan yang berkembang pesat dan memiliki aktivitas yang semakin beragam, Divisi TI PT. Bank XYZ Surabaya dihadapkan dengan risiko yang semakin kompleks. Risiko-risiko tersebut terkait dengan keamanan informasi, dimana informasi merupakan aset penting yang harus dilindungi keamanannya dari pihak yang tidak berwenang yang akan menggunakannya untuk kepentingan tertentu atau akan merusak informasi tersebut. Oleh karenanya, untuk mengantisipasi kemungkinan terjadinya risiko tersebut maka dilakukan penilaian risiko. Untuk melakukan penilaian risiko pada penelitian ini menggunakan penerapan metode FMEA (Failure Mode & Effects Analysis), yaitu suatu metodologi yang digunakan untuk mengidentifikasi dan mengevaluasi kegagalan potensial, menentukan tingkatan resiko dari kegagalan dan skala prioritas untuk mengambil tindakan yang diperlukan. Makalah ini menghasilkan Risk Register, yaitu daftar analisis risiko yang dapat digunakan sebagai acuan oleh Divisi TI PT. Bank XYZ Surabaya dalam merumuskan tata kelola untuk melindungi keamanan informasinya.

Kata kunci: *Risiko Teknologi Informasi, Penilaian Risiko, Mitigasi Risiko, Keamanan Informasi, Metode FMEA*

Abstract

As a financial institution that is growing rapidly and has an increasingly diverse business activities, IT Division of PT. XYZ Bank is faced with an increasingly complex risks. One of risks is the risks related to information security, where information is a very important asset that its security must be protected from unauthorized parties who will use it for such purposes or to destroy such information. Therefore, to anticipate the likelihood of such risks, a risk assessment is needed. To identify risks, this research uses FMEA method (Failure Mode & Effects Analysis), which is a methodology used to identify and evaluate potential failure, determine the level of risk of failure and priority to take the necessary action. At the end of this paper, a risk register that contains a list of risks is presented. The risk register is expected to be used as a reference to propose the governance in order to protect the information security of IT Division PT. XYZ Bank Surabaya.

Keywords: *Information Technology Risk, Risk Assessment, Risk Mitigation, Information Security, FMEA Method*

1. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) saat ini banyak memberikan kemudahan pada berbagai aspek kegiatan bisnis [1]. Peranan TI sebagai pendukung proses bisnis bagi suatu organisasi sudah semakin penting. Teknologi Informasi (TI) merujuk pada teknologi yang digunakan dalam menyampaikan maupun mengolah informasi. Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Informasi yang bernilai penting tersebut merupakan aset bagi organisasi sehingga harus dilindungi keamanannya [2]. Selain memberikan keuntungan bagi perusahaan, TI juga menimbulkan risiko yang beragam, misalnya kehilangan data yang disebabkan adanya virus dan kesalahan yang terjadi karena faktor kesengajaan atau kecurangan. Risiko-risiko tersebut akan menimbulkan dampak kerugian yang besar bagi perusahaan, baik secara *financial* maupun non *financial*. Salah satu perusahaan yang menggunakan teknologi informasi (TI) sebagai bagian yang penting dalam mendukung tujuan dan sasaran bisnisnya adalah pada sektor perbankan. PT. Bank XYZ Surabaya merupakan salah satu bank nasional terbesar di Indonesia yang berkantor pusat di Surabaya yang memberikan pelayanan terbaik terhadap nasabahnya. Banyaknya aktivitas proses bisnis yang dilakukan, sehingga

membuat TI sangat rentan terhadap keamanan informasi. Pada Divisi TI yang menggunakan perkembangan teknologi informasi untuk menunjang proses bisnisnya, pada kenyataannya ini membuat jalannya proses bisnis perbankan menjadi semakin mudah, akan tetapi di sisi yang lain ini juga membuat semakin berisiko dan ancaman terhadap keamanan informasi perbankan semakin meningkat dari hari ke hari.

Oleh karena itu, untuk meningkatkan perlindungan terhadap aset informasi, maka perlu dilakukan penilaian risiko keamanan informasi. Metode yang digunakan dalam penilaian risiko tugas akhir ini yaitu metode FMEA (*Failure Mode & Effect Analysis*) [3]. Metode FMEA adalah suatu metodologi yang digunakan untuk mengidentifikasi dan mengevaluasi kegagalan potensial, menentukan tingkatan resiko dari dari kegagalan dan skala prioritas untuk mengambil tindakan yang dipelukan. Hasil dari penelitian ini adalah dokumen manajemen risiko yang didalamnya terdapat Risk Register, yaitu laporan hasil pengelolaan manajemen risiko yang berisikan daftar analisis risiko dan disertai pengendalian risiko yang dapat digunakan sebagai acuan untuk menangani setiap permasalahan keamanan informasi yang terjadi di Divisi TI PT. Bank XYZ Surabaya.

2. TINJAUAN PUSTAKA

Kajian pustaka ini berisi literatur yang digunakan sebagai acuan penelitian serta teori penelitian sebelumnya yang berhubungan dengan permasalahan penelitian ini. Kajian yang dibahas dalam bab ini antara lain adalah Sekilas PT. Bank XYZ, Definisi Aset, Aspek Keamanan Informasi, Ancaman Keamanan Informasi, , Manajemen Risiko, dan Metode FMEA (*Failure Mode & Effects Analysis*).

2.1 Sekilas Divisi TI PT. Bank XYZ Surabaya

Divisi TI pada PT. Bank XYZ Surabaya bertanggung jawab terhadap kegiatan perencanaan, pengembangan, operasional, dan pemantauan TI secara menyeluruh untuk mendukung aktivitas bank. Pada struktur organisasi Divisi TI PT. Bank XYZ dibagi menjadi tiga Sub Divisi yaitu Sub Divisi Strategi dan Keamanan TI, Sub Divisi Pengembangan TI, dan Sub Divisi Dukungan dan Operasional TI.

2.2 Definisi Aset

Istilah aset informasi mengacu pada elemen data aktual, catatan, file, sistem perangkat lunak (aplikasi), dan sebagainya.Sedangkan istiah aset TI mengacu pada sekumpulan aset yang lebih luas termasuk perangkat keras, media, elemen-elemen komunikasi, dan lingkungan TI yang sebenarnya dari perusahaan. Istiah umum aset mengacu pada baik aset informasi maupun aset TI [4].

2.3 Aspek Keamanan Informasi

Organisasi keamanan informasi memiliki tiga aspek yang harus dipahami untuk bisa menerapkannya, aspek tersebut biasa disebut dengan CIA Triad Model [5], yang antara lain adalah:

- *Confidentiality* (kerahasiaan). Merupakan aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
- *Integrity* (integritas). Merupakan aspek yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi.
- *Availability* (ketersediaan). Merupakan aspek yang menjamin bahwa data akan tersedia saat dibutuhkan kapanpun dan dimanapun, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait

2.4 Ancaman Keamanan Informasi

Threat atau ancaman adalah suatu potensi yang disebabkan oleh insiden yang tidak diinginkan yang mungkin membahayakan jalannya proses bisnis organisasi [2]. Ancaman-ancaman SI/TI tersebut diantaranya[6]:

- *Compromises to intellectual property* (pembajakan, pelanggaran hak cipta)
- *Espionage* atau pelanggaran (akses yang tidak sah dan/atau pengumpulan data)
- *Forces of nature* (kebakaran, banjir, gempa bumi, petir)
- *Human error or failure* (kecelakaan, kesalahan karyawan, *failure to follow policy*)
- *Information extortion* (*blackmail of information disclosure*)
- *Missing, inadequate, or incomplete controls* (kontrol perangkat lunak, keamanan fisik)
- *Missing, inadequate, or incomplete organizational policy or planning* (masalah pelatihan, privasi, kurangnya kebijakan yang efektif)
- *Dan lain-lain*

2.5 Manajemen Risiko

Risiko adalah sebagai kemungkinan terkena kerusakan atau kerugian. Hal ini mengacu pada situasi dimana seseorang bisa melakukan sesuatu yang tidak diinginkan atau kejadian alam dapat menyebabkan hasil yang tidak diinginkan, yang menghasilkan dampak negatif [6]. Risiko dapat memberikan dampak yang cukup signifikan bagi organiasasi. Sebagai contoh adalah resiko yang muncul akibat perusahan menerapkan TI. Resiko yang mengikuti penerapan TI tersebut dapat berupa kerusakan atau ancaman lain bagi perangkat keras TI, perangkat lunak, maupun services yang ditawarkan oleh TI tersebut.

Manajemen resiko merupakan serangkaian aktivitas dalam menganalisis resiko. Resiko tersebut diidentifikasi, dinililai, dan selanjutnya disusun langkah strategis yang dapat digunakan dalam mengatasi resiko tersebut [7]. Proses pelaksanaan manajemen resiko, ketika memasuki tahapan penanganan atau aksi apa yang harus diambil, maka terdapat empat pilihan penanganan terhadap risiko potensial tersebut, yaitu *take* (terima), *treat* (kurangi), *terminate* (hindari), *transfer*.

2.5 Metode FMEA

FMEA *(Failure Mode and Effect Analysis)* adalah suatu prosedur terstruktur untuk mengidentifikasi dan mencegah sebanyak mungkin mode kegagalan *(failure modes)*. Langkah-langkah dalam pembuatan FMEA adalah sebagai berikut [3]:

- Me*review* proses.
- Brainstorm risiko potensial.
- Membuat daftar risiko, penyebab, dan efek potensial.
- Menentukan tingkat *severity*, yaitu suatu penilaian tingkat keparahan dari keseriusan *effect* yang ditimbulkan dari mode-mode kegagalan (*failure mode*), menghitung seberapa besar dampak/intensitas kejadian mempengaruhi output proses, maupun proses-proses selanjutnya.
- Menentukan tingkat *occurrence*, yaitu suatu penilaian mengenai peluang (probabilitas) frekuensi penyebab mekanisme kegagalan yang akan terjadi, sehingga dapat menghasilkan bentuk/mode kegagalan yang memberikan akibat tertentu selama masa penggunaan produk.
- Menentukan tingkat *detection*, yaitu pengukuran terhadap kemampuan mengendalikan/mengontrol kegagalan yang dapat terjadi.
- Menghitung RPN (*Risk Priority Number*), yaitu hasil perkalian *severity* (S), *occurrence* (O), dan *detection* (D). Kriteria RPN ditunjukkan pada tabel di bawah ini:

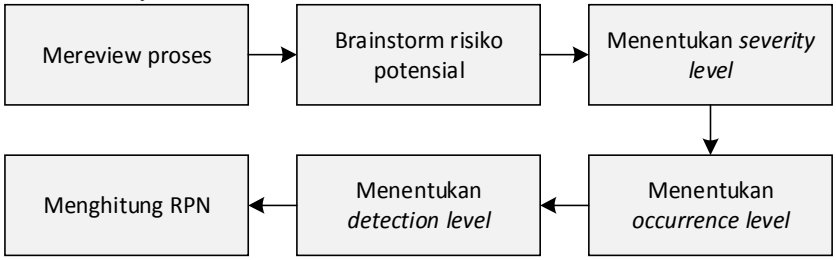
Tabel 38. Tabel Kriteria RPN

RPN	*Calculation Level*
0-19	*Very Low*
20-79	*Low*
80-119	*Medium*
120-199	*High*
≥200	*Very High*

- Membuat prioritas risiko untuk ditindaklanjuti.
- Mengambil tindakan untuk mengurangi atau menghilangkan risiko tertinggi / risiko kritis.

3. METODE PENELITIAN

Langkah-langkah penelitian dengan berdasarkan pada metode FMEA adalah sebagai berikut, sesuai dengan penjelasan pada bab sebelumnya.



Gambar 26 Metode penelitian berdasar FMEA

4. PEMBAHASAN

Pada bagian ini membahas analisis risiko keamanan informasi di Divisi TI PT. Bank XYZ Surabaya dengan metode FMEA (*Failure Mode & Effects Analysis*).

3.1 Mereview Proses

Secara organisasi, Divisi TI berada di bawah Direktur Operasional. Pada Divisi TI dibagi menjadi tiga Sub Divisi yaitu Sub Divisi Strategi dan Keamanan TI, Sub Divisi Pengembangan TI, dan Sub Divisi Dukungan dan Operasional TI. Beberapa proses bisnis yang dilakukan oleh Divisi TI PT. Bank XYZ Surabaya adalah sebagai berikut:

a) Proses bisnis strategi dan keamanan TI
   - Mengelola akses pengguna *database*
   - Mengorganisir evaluasi terhadap *system security* TI

b) Proses bisnis pendukung TI
   - Melakukan *back-up database*
   - Melakukan pengadaan barang dan jasa bidang TI
   - Mengelola dan memantau ketersediaan jaringan dan infrastruktur

c) Proses bisnis pengembangan TI
   - Mengelola pengembangan aplikasi/sistem TI
   - Mengelola pelaksanaan *project*

Untuk melakukan penelitian pada tugas akhir ini, penilaian risiko dengan menggunakan pendekatan aset yang ada di Divisi TI PT. Bank XYZ. Aset-aset tersebut adalah:

Tabel 39. Tabel Daftar Aset

Aset	Penjelasan
Data	Data *office* Divisi TI
Hardware	PC, server, hard disk, flash disk, firewall
Software	Aplikasi perbankan dan aplikasi pendukung kegiatan perbankan (misalnya antivirus, aplikasi MS office, dll)
Network	Jaringan yang mengakses informasi (misalnya internet, dll), LAN, backbone
People	*User* divisi TI (misalnya *developer, operator, system administrator*)
E-Banking	ATM, SMS banking, internet banking

3.2 *Brainstorming* Risiko

Pada tahap ini dilakukan brainstorm risiko potensial dengan tujuan untuk mengetahui kegagalan yang dapat terjadi pada fungsi dalam sistem yang diterapkan. *Output* yang diperoeh adalah daftar risiko disertai dampak dan penyebab yang potensial pada aset di Divisi TI di PT. Bank XYZ. Pada tahap ini diperoleh 39 identifikasi risiko beserta penyebab dan dampaknya dari kategori risiko *hardware, software, people, data, network*, dan *e-banking*.

3.3 Menentukan *Severity*

Severity adalah langkah pertama untuk menganalisa risiko yaitu suatu penilaian tingkat keparahan dari keseriusan effect yang ditimbulkan dari mode-mode kegagalan *(failure mode)*, menghitung seberapa besar dampak/intensitas kejadian mempengaruhi output proses, maupun proses-proses selanjutnya. Hasil penilaian tingkat *severity* dari masing-masing risiko yang nantinya akan digunakan dalam menghitung RPN *(Risk Priority Number)*.

3.4 Menentukan *Occurrence*

Occurrence adalah suatu penilaian mengenai peluang (probabilitas) frekuensi penyebab mekanisme kegagalan yang akan terjadi, sehingga dapat menghasilkan bentuk/mode kegagalan yang memberikan akibat tertentu selama masa penggunaan produk. Hasil penilaian tingkat *occurrence* dari masing-masing risiko yang nantinya akan digunakan dalam menghitung RPN (*Risk Priority Number*).

3.5 Menentukan *Detection*

Nilai *detection* diasosiasikan dengan pengendalian saat ini. *Detection* adalah pengukuran terhadap kemampuan mengendalikan/mengontrol kegagalan yang dapat terjadi.Hasil penilaian tingkat *detection* dari masing-masing risiko yang nantinya akan digunakan dalam menghitung RPN (*Risk Priority Number*).

3.6 Menghitung RPN

Tahap ini merupakan perhitungan *Risk Priority Number* (RPN). Perhitungan ini dilakukan dengan cara pengkalian dari nilai *severity, occurrence*, dan *detection*. Dari proses penilaian tersebut akan dibobotkan sehingga didapatkan RPN yang merupakan skor potensi dari risiko-risiko yang telah diidentifikasi tersebut.

3.7 Membuat Prioritas Risiko

Pada tahap ini setelah risiko-risiko tersebut diukur tingkat *severity*, *occurrence*, dan *detection*, dilakukan susunan urutan prioritas risiko mulai dari risiko yang tertinggi sampai risiko yang terendah, seperti terlihat pada tabel berikut ini.

Tabel 40 Beberapa risiko yang teridentifikasi dan prioritasnya

Kategori	Risk ID	Identifikasi Risiko	Sev	Occ	Det	RPN	Level	Rank
People	PE002	Adanya suatu pekerjaan terkait TI di Divisi TI terhambat	6	4	5	120	*High*	1
People	PE004	Terjadinya *human error*	6	5	3	90	*Medium*	2
Software	SW004	Bocornya informasi *source code* aplikasi perbankan pada pihak lain atau kompetitor	8	3	3	72	*Low*	3
Network	NW005	*Misconfiguration core network*	8	4	2	72	*Low*	4
Network	NW007	Serangan *hacker*	9	2	4	72	*Low*	5
People	PE001	Ketergantungan terhadap karyawan	6	4	3	72	*Low*	6
People	PE003	Kebocoran informasi mengenai data penting bank ke pihak luar	9	4	2	72	*Low*	7
Network	NW005	Adanya gangguan *gateway*	8	4	2	64	*Low*	8
Hardware	HW001	Kerusakan pada server	5	3	4	60	*Low*	9
e-banking	EB003	Penipuan SMS banking	7	4	2	56	*Low*	10
e-banking	EB004	Terjadinya *phising* pada *internet banking*	7	4	2	56	*Low*	11
Data	DT003	Terjadinya *corrupt* atau eror pada data	6	3	3	54	*Low*	12
e-banking	EB002	Terjadi pembobolan pada mesin ATM	6	3	3	54	*Low*	13
Data	DT002	Data tidak ter-*backup*	7	3	2	42	*Low*	14
Software	SW001	Serangan virus	5	4	2	40	*Low*	15
e-banking	EB005	Akses ke internet banking lambat	5	4	2	40	*Low*	16
Hardware	HW002	Kerusakan pada PC	3	3	4	36	*Low*	17
Hardware	HW007	Server mesin *production* tidak berfungsi	8	2	2	32	*Low*	18
Network	NW001	Terjadi gangguan *backbone* pada data center	8	2	2	32	*Low*	19
Network	NW002	Terjadi gangguan *backup communication*	8	2	2	32	*Low*	21
Data	DT004	Penyalahgunaan atau modifikasi data	8	2	2	32	*Low*	23
Software	SW001	Serangan virus	5	3	2	30	*Low*	24
e-banking	EB001	Kerusakan mesin ATM	5	3	2	30	*Low*	25
Data	DT001	Data *overload*	7	2	2	28	*Low*	26
Hardware	HW001	Kerusakan pada server	5	2	2	20	*Low*	27

Risiko di atas diurutkan berdasarkan nilai RPN tertinggi. Sebagai contoh, risiko dengan ID PE002 memiliki nilai RPN 120 yang merupakan hasil pengalian dari *severity*, *occurrence* dan *detection*. Pengurutan risiko ini perlu dilakukan untuk menentukan dan memberikan panduan bagi pihak Divisi TI dalam penanganan risiko-risiko tersebut, yakni dengan memprioritaskan penanganan risiko yang memiliki potensi atau skor tertinggi.

4. SIMPULAN DAN SARAN

Pada bab ini merangkum hasil akhir dari penelitian ini menjadi sebuah kesimpulan dan dilengkapi dengan saran-saran untuk perbaikan ataupun penelitian lanjutan.

4.1 Simpulan

Berdasarkan hasil penelitian, berikut ini merupakan beberapa kesimpulan yang dapat diambil:

1. Dari proses identifikasi risiko yag terdapat pada aset Divisi TI diperoleh beberapa risiko yang dikategorikan berdasarkan *hardware, software, network, data, people* dan *e-banking*.
2. Penilaian risiko dengan metode FMEA dilakukan melalui beberapa tahapan yaitu me*review* proses, brainstorm risiko, menentukan tingkat *severity*, menentukan tingkat *occurrence*, menentukan tingkat *detection*, menghitung RPN (*Risk Priority Number*), membuat prioritas risiko, dan mitigasi risiko (tindakan yang bisa diambil untuk mencegah atau mengurangi kesempatan terjadinya potensi kegagalan atau pengaruh pada sistem). Dari proses penilaian risiko menggunakan metode FMEA didapatkan risiko yang mempunyai skor *assessment* tertinggi hingga terendah. Untuk risiko *high* dengan nilai RPN sebesar 120, yaitu pada kategori risiko *people* dengan identifikasi risiko adanya suatu pekerjaan terkait TI di Divisi TI terhambat, dengan penyebab *resource* yang terbatas.

4.2 Saran

Makalah ini belum memaparkan mengenai tindakan mitigasi dan kontrol dari risiko yang telah teridentifikasi. Oleh karenanya, saran yang dapat dijadikan acuan dalam pengembangan makalah selanjutnya yakni menentukan mitigasi dan kontrol berdasarkan standard keamanan informasi. Selanjutnya, kontrol tersebut juga dapat dijadikan sebagai dasar dalam pembuatan dokumen prosedur dan tata kelola lain dalam rangka menjaga keamanan informasi.

5. DAFTAR RUJUKAN

[1] Raymond McLeod, Jr. 1997. *Management Information System*. Prentice Hall Inc. Englewood Cliffs. New Jersey.
[2] Sarno, R. dan Iffano. 2009. *Sistem Manajemen Keamanan Informasi Berbasis ISO 27001*. Surabaya: ITS Press.
[3] Mcdermott, Robin E., Mikulak, Raymond J., Beauregard, Michael R. 1996. *The Basic of FMEA*. New York: 444 Park Avenue South, 7th floor.
[4] Firesmith, D.G. 2003. *Common Concept Underlying Safety, Security, and Survivability Engineering*.
[5] Whitman, E. & Mattord, H. 2011. *Principles of Information Security*, 4th edition.
[6] Christopher Alberts, A. D. 2002. *Managing Information Security Risks: The OCTAVE Approach.*
[7] Harahap et.al. 2010. *Pengukuran Risiko manajemen Proyek Teknologi Informasi.*