ANALISIS MANAJEMEN RISIKO TI PEMELIHARAAN ASET MENGGUNAKAN *QUANTITATIVE RISK ANALYSIS* (QRA) PADA PT. HMS

Agung Yulianto[1)], Awalludiyah Ambarwati [2)], Cahyo Darujati [3)]

[1,2,3)] Program Studi Sistem Informasi, Fakultas Ilmu Komputer,
Universitas Narotama, Jl. Arief Rahman Hakim No 51 Sukolilo, Surabaya

e-mail: ambarwati1578@yahoo.com

Abstract

Role of Information Technology (IT) in the company is an important element to support the effectiveness and efficiency of business processes. IT assets is a critical component in the company's business processes. They are vulnerable to the risks that may occur. Malfunction of IT assets due to threat/risk may disrupt the company's performance systematically. IS Service Management Department at PT. HMS is responsible for managing the company's IT assets. In this research, IT assets focus on hardware consisting of Mobile Device (Tab, iPhone and iPad), Notebook (Laptop), Desktop (CPU) and Monitor with a considerable quantity and stored in four different warehouse locations. Management needs to identify risk factors that need priority maintenance as well as the type of IT assets anywhere that needs special attention. IT risk management analysis is conducted to identify and measure IT assets using Quantitative Risk Analysis (QRA) methods in order to find aspects and factors that require particular attention effectively and efficiently. As result, it recommended kinds of IT assets such as laptops and type of risk factors for accidental errors that require priority for further control measures taken by the management company.

Keywords: IT asset hardware, QRA, risk analysis

Abstrak

Peranan Teknologi Informasi (TI) didalam perusahaan merupakan suatu elemen penting untuk menunjang efektifitas dan efisiensi proses bisnis perusahaan. Aset TI adalah komponen penting dalam proses bisnis perusahaan yang memiliki kerentanan terhadap risiko yang mungkin terjadi. Ketidakfungsian dari aset TI karena ancaman/risiko dapat mengganggu kinerja perusahaan secara sistematis. Department IS Service Management pada PPT. HMS bertanggung jawab dalam mengelola aset TI perusahaan. Aset TI yang menjadi obyek dari penelitian mencakup perangkat keras yang terdiri dari Mobile Device (Tab, IPhone dan IPad), Notebook (Laptop), Desktop (CPU) dan Monitor dengan kuantitas yang cukup banyak dan tersimpan dalam empat lokasi gudang. Berangkat dari kebutuhan manajemen dalam mengidentifikasi faktor risiko yang perlu mendapat prioritas pemeliharaan serta jenis aset TI mana saja yang perlu mendapat perhatian khusus. Untuk memenuhi kebutuhan tersebut, dilakukan analisa manajemen risiko TI guna mengidentifikasi dan mengukur aset TI menggunakan metode Quantitative Risk Analysis (QRA) sehingga dapat diketahui aspek dan faktornya yang memerlukan perhatian khusus secara efektif dan efisien. Penelitian ini menghasilkan rekomendasi jenis aset TI berupa Laptop dan jenis faktor risiko kesalahan tidak disengaja yang memerlukan prioritas untuk diambil tindakan pengendalian lebih lanjut oleh manajemen perusahaan.

Kata Kunci : aset TI perangkat keras, QRA, analisa risiko.

PENDAHULUAN

Peranan Teknologi Informasi (TI) di dalam perusahaan merupakan suatu elemen penting untuk menunjang efektifitas dan efisiensi proses bisnis perusahaan. Penerapan TI dapat meningkatkan mutu pelayanan sehingga tercapainya tujuan bisnis perusahaan. Pemanfaatan TI harus diiringi dengan pengelolaan yang tepat dan relevan sehingga dapat meminimalisasi risiko-risiko yang mungkin timbul di dalam proses bisnis.

Fungsi TI tidak hanya sebagai fasilitas pendukung utama, tetapi juga dapat menjadi *critical success factor* dalam suatu industri *manufacturing* seperti halnya pada PT. HMS, yang telah menggunakan dan memanfaatkan TI dalam menjalankan proses bisnisnya selama bertahun-tahun. Department IS Service Management merupakan suatu departemen pada PT. HMS, yang memberikan pelayanan kepada semua pengguna aset TI. Bagian Aset dalam Department IS Service Management berperan penting dalam menjalankan roda bisnis. Namun, perusahaan belum melakukan identifikasi risiko implementasi TI secara berkala dan terperinci.

Pemeliharaan aset TI yang salah dapat menimbulkan risiko–risiko untuk Department IS Service Management. Untuk menghindari hal tersebut diperlukan manajemen risiko untuk meminimalkan risiko yang dapat terjadi dan membuat rekomendasi bagi manajemen PT. HMS dalam pemeliharaan aset TI yang dimiliki. Penelitian ini bertujuan untuk melakukan analisa manajemen risiko TI pemeliharaan aset menggunakan *Quantitative Risk Analysis* (QRA) pada PT. HMS.

Menurut Peltier (2001, p. 224) Manajemen risiko adalah suatu proses identifikasi, mengatur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Strategi yang dapat digunakan antara lain: mentransfer risiko pada pihak lain, menghindari risiko, mengurangi efek buruk dari risiko, dan menerima sebagian maupun seluruh konsekuensi dari risiko tertentu.

J. W. Meritt (2000) menyatakan bahwa dalam analisa risiko terdapat dua metode utama dan satu metode *hybrid*. Pertama, Metode Analisis Kualitatif (*Qualitative Analysis Method*), yaitu metode analisis risiko yang menggunakan tabulasi berdasarkan penilaian deskriptif (tinggi, sedang atau rendah). Kedua, Metode Analisis Kuantitatif (*Quantitative Analysis Method*), yaitu metode analisis risiko yang menggunakan angka numerik untuk menyatakan dampak dan probabilitas. Yang terakhir adalah *Hybrid method* yang merupakan kombinasi dari Metode Analisis Kualitatif dan Metode Analisis Kuantitatif.

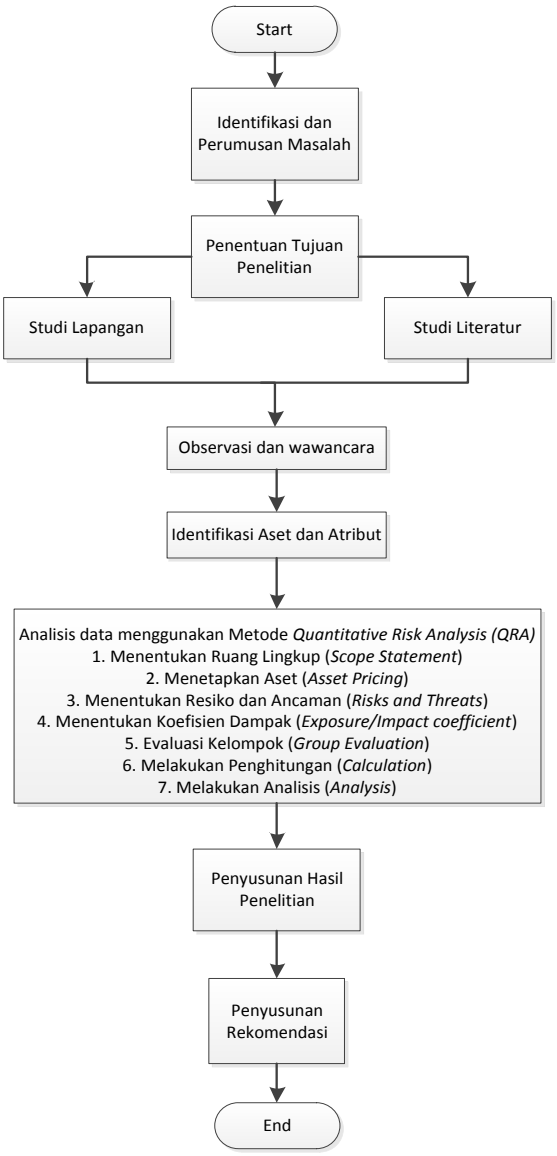
Aset Teknologi Informasi (Aset TI) merupakan barang yang dinilai oleh suatu perusahaan atau organisasi yang dapat memberikan manfaat pada kegiatan operasional pada perusahaan, yang berwujud maupun yang tidak berwujud dan dijadikan sebagai modal perusahaan atau organisasi (Rully Anthony, 2008). Ding Tan (2002) membagi, Aset TI berdasarkan segi manfaat yang dirasakan berupa *IT Asset Tangible* dan *IT Assets Intangible*.

IT Asset Tangible, yaitu aset pada perusahaan yang bermanfaat bagi perusahaan atau *user* yang secara nyata dapat langsung diaplikasikan untuk keuntungan pribadi maupun bersama seperti *hardware, database*, server, komputer. Sedangkan *IT Assets Intangible* adalah aset pada perusahaan yang bermanfaat bagi perusahaan maupun bagi *user* yang secara tidak nyata dapat diperoleh manfaatnya seperti *software application, security program,* dan *license software.* Aset TI pada penelitian ini merupakan *IT Asset Tangible* meliputi *Desktop*, Laptop, *Mobile Device* dan Monitor.

METODE

Penelitian ini dilakukan menggunakan metode *Quantitative Risk Analysis* (QRA) menurut J. W. Meritt (2000) meliputi tujuh tahapan antara lain :

a. Menentukan Ruang Lingkup (*Scope Statement*)
b. Menetapkan Aset (*Asset Pricing*)
c. Resiko dan Ancaman (*Risks and Threats*)
d. Menentukan Koefisien Dampak (*Exposure/Impact coefficient*)
e. Evaluasi Kelompok (*Group Evaluation*)
f. Melakukan Penghitungan (*Calculation*)
g. Melakukan Analisis (*Analysis*)



Gambar 1. Diagram Alur Tahapan Penelitian

Penentuan ruang lingkup (*scope statement*) perlu memperhatikan tiga hal. Pertama, menentukan secara tepat obyek yang dievaluasi dalam hal ini lokasi dan jumlah aset TI yang dianalisa. Lokasi berupa empat gudang yang terletak di Sukorejo Pandaan, Kalirungkut Surabaya, Karawang dan OPP Jakarta. Jumlah Aset TI yang dianalisa adalah aset TI pada periode bulan Januari 2016 sampai dengan bulan Juli 2016 dengan tipe dan model Aset TI meliputi *Desktop*, Laptop, *Mobile Device* dan Monitor. Berikutnya adalah penentuan metode analisa risiko, yaitu *Quantitative Risk Analysis* (QRA).

Terakhir melakukan kalkulasi analisis untuk menentukan aspek yang perlu untuk dilakukan pengendalian.

Penetapan aset (*asset pricing*) dilakukan dengan menentukan harga (*price*) sesuai dengan tipe dan model aset TI yang dianalisa dari sumber *database* Aset TI (*Service-Now*) perusahaan. Menentukan Risiko (*Risk*) dan Ancaman (*Threats*) dengan tujuan untuk mengidentifikasi potensi dari sumber ancaman dan melakukan penyusunan suatu daftar yang memaparkan ancaman potensi sumber ancaman sehingga dapat diterapkan pada sistem pemeliharaan aset TI yang sedang dievaluasi. Suatu sumber ancaman digambarkan sebagai suatu keadaan atau peristiwa yang memiliki potensi dapat menyebabkan kerusakan pada suatu sistem pemeliharaan aset TI.

J. W. Meritt (2000) membuat kategori ancaman (*Threats*) menjadi 15 macam antara lain :

a. *Power loss* (Kehilangan Daya), hilangnya pasokan daya listrik ke sistem informasi yang mengakibatkan terganggunya fungsi aset TI.
b. *Communication Loss* (Kehilangan Komunikasi), ketidakmampuan untuk mentransfer informasi ke/dari sistem.
c. *Data Integrity Loss* (Kehilangan Integeritas Data), kehilangan keabsahan dari suatu data merupakan kerugian yang tinggi bagi pengguna sebagai aset TI.
d. *Accidental Errors* (Kesalahan Tidak Disengaja), penyalahgunaan aset TI bukan karena niat jahat, tetapi karena terjadi kesalahan dalam penggunaannya yang mengakibatkan kerugian bagi perusahaan.
e. *Computer Virus*, kerugian diakibatkan oleh virus komputer yang membuat aset TI menjadi berkurang hingga kehilangan fungsinya.
f. *Abuse of Access Privileges by Employees* (Penyalahgunaan Hak Akses oleh Karyawan), meliputi tindakan yang dapat dilakukan oleh karyawan tetapi yang tidak berwenang.
g. *Natural disasters* (Bencana Alam), kejadian yang menurunkan beberapa aspek dari aset TI berupa, banjir, angin puyuh, petir, dan lain-lain.
h. *Attempted Unauthorized System Access by Outsider* (Usaha Orang luar yang masuk ke sistem), meliputi orang lain yang bukan karyawan yang mencoba memasuki sistem tetapi tidak berhasil.
i. *Theft or Destruction of Computing Resource* (Pencurian atau penghancuran aset TI), meliputi pengguna yang tidak sah yang melakukan penghancuran/pencurian terhadap aset TI.
j. *Destruction of Data* (Penghancuran Data), meliputi hal-hal yang dapat merusak informasi/data perusahaan atau hanya mencegah perusahaan untuk menggunakannya.
k. *Abuse of Access Privileges by Other Authorized User* (Penyalahgunaan Hak Akses oleh Pengguna lain), meliputi pengguna lain yang berwenang melakukan operasi namun disalahgunakan.
l. *Successful Unauthorized System Access by Outsider* (Pihak luar yang berhasil akses ke sistem), meliputi bukan pengguna yang sah dan berhasil memasuki sistem, dengan istilah lain yaitu *hacker*.
m. *Non-disaster downtime* (Penghentian proses tanpa bencana), meliputi saat-saat ketika sistem informasi tidak tersedia untuk digunakan tetapi tidak disebabkan oleh bencana.
n. *Fire*/Kebakaran.
o. *Earthquake* (Gempa bumi).

Menentukan Koefisien Dampak (*Exposure/Impact coefficient*) diperlukan tahapan identifikasi dimana aset memiliki kerentanan terhadap risiko tertentu atau yang tidak sama sekali terhadap suatu risiko dengan melakukan klasifikasi dampak pada aset TI berdasarkan tingkat *vulnerability* (kerentanan atau kelemahan) aset TI tersebut. *Vulnerability Analysis*/Analisa Kerentanan aset TI dilakukan untuk mengetahui potensi kehilangan aset, yang disebut *Exposure Factor* (EF), yang merupakan presentase kehilangan akibat ancaman yang terjadi terhadap aset.

Evaluasi Kelompok (*Group Evaluation*) dilakukan untuk mengulas ancaman (*threat*) dan koefisiensi dampak EF (*Exposure Factor*) pada aset TI. Kelompok ini terdiri dari Manager Departemen IS Service Management, Manager EHS (*Environment, Healthy, Safety*), Manager Power Plant, Manager IS Security, Manager NSD (*Nasional Security Departement*), dan Manager Jaringan (*Network*).

Melakukan Penghitungan (*Calculation*) *Impact Analysis* (perhitungan terhadap dampak dari kejadian gangguan keamanan) berupa *Single Loss Expectancy* (SLE) dan *Annualized Loss Expectancy* (ALE).

Single Loss Expectancy (SLE) yaitu nilai moneter yang akan hilang pada satu kali kejadian gangguan keamaan informasi. Rumus dalam mencari SLE :

$$SLE = \text{Asset Value} \times EF \quad (1)$$

Dimana

Asset Value : merupakan nilai finansial masing-masing aset TI yang telah ditetapkan nilainya dalam tahapan ke 2, *Asset Pricing*.

EF : *Exposure Factor*, merupakan presentase kehilangan akibat ancaman yang terjadi terhadap aset

Annualized Loss Expectancy (ALE) yaitu nilai moneter yang akan hilang karena gangguan keamanan

ISSN (2540-9700)

terhadap aset, pada jangka waktu satu tahun. Rumus dalam mencari ALE :

ALE = SLE x ARO (2)

Dimana

SLE : *Single Loss Expectancy*, merupakan nilai kerugian secara finansial pada setiap aset TI yang diakibatkan oleh setiap *threat*.

ARO : *Annualized Rate Occurrence*, merupakan nilai prosentase potensi setiap *threat* untuk setiap aset TI dalam 1 tahun.

Tahap terakhir berupa analisis yang dapat menghasilkan dan menentukan aspek mana yang patut mendapatkan pengendalian. Menurut James W. Merrit (2000) dalam tahapan analisis terdapat dua metode yaitu *Analysis Across Asset* dan *Analysis Across Risk*. Melakukan *Analysis Across Asset* dengan cara menjumlahkan nilai dampak masing-masing aset TI dari semua *threat* dari *spreadsheet* pada tahapan kalkulasi dan menentukan skala prioritas jenis aset TI yang perlu mendapatkan pengendalian. Sedangkan *Analysis Across Risk* dilakukan dengan cara menjumlahkan nilai dampak masing-masing threat untuk semua aset TI dari *spreadsheet* pada tahapan kalkulasi dan menentukan skala prioritas jenis *threat*/risiko yang perlu mendapatkan pengendalian.

Sumber data primer didapat melalui observasi dan pengamatan di area kerja serta hasil wawancara yang dilakukan kepada Manager Service Management, Supervisor Asset Management, Staf Asset Management dan Staf GRASP (General PC Replacement, Additional, Spare and Project). Sedangkan data sekunder diperoleh dari perusahaan berupa peraturan dan standar yang berlaku diperusahaan, prosedur kerja, diagram alir, data aset TI, profil perusahaan, struktur organisasi, serta dokumen penunjang lain.

HASIL DAN PEMBAHASAN

Lokasi penelitian berupa empat gudang PT. HMS yang terletak di Sukorejo Pandaan, Kalirungkut Surabaya, Karawang dan OPP Jakarta. Jumlah Aset TI yang dianalisa adalah aset TI pada periode bulan Januari 2016 sampai dengan bulan Juli 2016 dengan tipe dan model Aset TI meliputi *Desktop*, Laptop, *Mobile Device* dan Monitor. Obyek penelitian berfokus kepada aset TI yang bersifat *equipment* dan bernilai *tangible*.

Tabel 1. Daftar 4 tipe Aset TI

Tipe Aset TI	Jumlah Aset TI (Unit)
Desktop	481
Laptop	675
Mobile Device	459
Monitor	324

Sumber : Dokumen IT Aset PT. HMS, diolah kembali

Desktop, laptop dan monitor yang dipergunakan perusahaan terdiri dari satu merek dengan beberapa varian. Sedangkan *mobile device* terdiri dari beberapa merek dan beberapa varian untuk setiap merek.

Menentukan Risiko dan Ancaman dengan memberikan nilai ARO (*Annualize Rate Occurance*) pada setiap jenis ancaman (Tabel 3). ARO diperoleh dari nilai prosentase potensi setiap *threat* untuk setiap aset TI dalam 1 tahun pada PT. HMS yang telah didokumentasikan oleh Department IS Service Management.

Tabel 2. Penetapan Harga Aset TI (*Asset Pricing*)

Asset Type	**Jumlah**	**Total Harga (Rp)**
Desktop	481	Rp 4,375,319,000
Laptop	675	Rp 9,232,080,000
Mobile Device	459	Rp 4,474,574,000
Monitor	324	Rp 710,502,000
Jumlah		**Rp 18,792,475,000**

Sumber : Dokumen IT Aset PT. HMS, diolah kembali

Tabel 3. Ancaman dalam satu tahun

Ancaman (Threat)	**ARO**
Kerugian Daya *(Power loss)*	2
Kerugian Komunikasi	2
Kesalahan tidak disengaja	0.72
Virus Komputer	0.68
Penyalahgunaan Hak Akses Karyawan	0.4
Bencana Alam *(Natural Disasters)*	0.29
Pencurian atau penghancuran aset TI	0.24
Pihak luar yang berhasil akses ke sistem	0.08
Penghentian proses tanpa bencana	0.06
Kebakaran *(Fire)*	0.01

Sumber : Dokumen IT Aset PT. HMS, diolah kembali

Menentuan koefisien dampak terhadap tingkat *vulnerability* (kerentanan) aset TI, dengan nilai kerentanan antara 0-100% (Tabel 4). Nilai koefisien dampak pada aset TI diperoleh dari Merrit (2000).

Tabel 4. Nilai Koefisien Dampak pada aset TI

Nilai	**Diskripsi**
0	Aset TI tersebut tahan dan tidak ada hasil kerusakan terhadap ancaman.
0.3	Tidak ada kerusakan yang diakibatkan namun ada kemungkinan membutuhkan penggantian total.
0.5	Kemungkinan tidak ada kerusakan yang dihasilkan pada aset TI.
0.7	Aset TI yang terkena dampak biasanya akan memerlukan penggantian.
1	Hasil yang dapat diidentifikasi adalah penggantian secara total pada aset TI.

Sumber : Merrit (2000)

Tabel 5 menunjukkan bahwa nilai koefisien dampak tertinggi yang terjadi pada aset TI adalah dari threat/risiko Pencurian atau penghancuran aset TI. Sedangkan untuk aset TI dengan jenis Monitor yang mempunyai koefisiensi

dampak yang berbeda dengan aset TI *Desktop*, Laptop dan *Mobile Device*. Koefisien dampak pada aset TI Monitor terdapat pada Tabel 6 Koefisien Dampak pada aset TI Monitor.

Koefisien Dampak pada aset TI Monitor mempunyai nilai yang berbeda dibandingkan dengan pada aset TI *Desktop*, Laptop dan *Mobile Device*, terutama terhadap threat Kerugian Komunikasi, Virus Komputer dan Penyalahgunaan Hak Akses oleh Karyawan, karena Monitor tidak rentan terhadap 3 *threat* tersebut.

Tabel 5. Koefisien Dampak pada aset TI

No	Ancaman (*Threat*)	EF
1	Kerugian Daya (*Power loss*)	0.1
2	Kerugian Komunikasi (*Communication Loss*)	0.1
3	Kesalahan tidak disengaja (*Accidental Errors*)	0.5
4	Virus Komputer	0.1
5	Penyalahgunaan Hak Akses oleh Karyawan	0.2
6	Bencana Alam (*Natural Disasters*)	0.5
7	Pencurian atau penghancuran aset TI	1
8	Pihak luar yang berhasil akses ke sistem	0.7
9	Penghentian proses tanpa bencana (*Non-disaster downtime*)	0.2
10	Kebakaran (*Fire*)	0.5

Sumber : Hasil Evaluasi Kelompok, diolah kembali

Tabel 6. Koefisiensi Dampak pada aset TI Monitor

No	Ancaman (Threat)	EF
1	Kerugian Daya (*Power loss*)	0.1
2	Kerugian Komunikasi (*Communication Loss*)	0
3	Kesalahan tidak disengaja (*Accidental Errors*)	0.5
4	Virus Komputer	0
5	Penyalahgunaan Hak Akses oleh Karyawan	0
6	Bencana Alam (*Natural Disasters*)	0.5
7	Pencurian atau penghancuran aset TI	1
8	Pihak luar yang berhasil akses ke sistem	0.5
9	Penghentian proses tanpa bencana (*Non-disaster downtime*)	0.2
10	Kebakaran (*Fire*)	0.5

Sumber : Hasil Evaluasi Kelompok, diolah kembali

Penghitungan dilakukan dalam dua langkah. Pertama, membuat *spreadsheet* dan memasukkan nilai (*value*) aset TI pada sumbu vertikal yang didapatkan dari Tabel 2 Penetapan Harga Aset TI (*Asset Pricing*). Kemudian memasukkan nilai *threat* pada sumbu horizontal yang didapatkan dari tabel Tabel 3 Ancaman dalam satu tahun. Selanjutnya, masukkan nilai koefisien dampak (EF) diantaranya nilai aset TI dan nilai *threat*. Memasukkan nilai Koefisien Dampak untuk aset TI *Desktop*, Laptop dan *Mobile Device* didapatkan dari Tabel 5, sedangkan nilai untuk Koefisiensi Dampak pada aset TI Monitor didapatkan dari Tabel 6. Deskripsi *spreadsheet* Nilai Aset TI, Nilai Threat dan Nilai Koefisien Dampak/*Exposure Factor* (EF) terdapat pada Tabel 7.

Langkah kedua yaitu membuat *spreadsheet* yang berbeda kemudian mengisi nilai pada masing-masing *cell* dari hasil perkalian antara nilai aset TI, nilai *threat* dan nilai koefisien yang didapatkan dari Tabel 7 Nilai Aset TI, Nilai Threat dan Nilai Koefisien Dampak dengan hasil pada Tabel 8 Kalkulasi Nilai Koefisien Dampak dalam nilai Finansial (Rupiah).

Tabel 8 menjelaskan bahwa ancaman/risiko mempunyai dampak kerugian finansial yang besar jika terjadi aset TI perusahaan. Hanya pada aset TI berjenis Monitor yang tidak terpengaruh pada jenis threat Kehilangan Komunikasi, Virus Komputer dan Penyalahgunaan Hak Akses oleh Karyawan.

Tabel 7. Nilai Aset TI, Nilai *Threat* dan Nilai Koefisien Dampak

	Tipe Aset TI	Desktop	Monitor	*Mobile Device*	Laptop
	Nilai Aset TI	Rp 4,375,319,000	Rp710,502,000	Rp 4,474,574,000	Rp 9,232,080,000
Ancaman (Threat)	**Risiko**				
Kehilangan Daya *(Power loss)*	2	0.1	0.1	0.1	0.1
Kehilangan Komunikasi	2	0.1	0	0.1	0.1
Kesalahan tidak disengaja	0.72	0.5	0.5	0.5	0.5
Virus Komputer	0.68	0.5	0	0.5	0.5
Penyalahgunaan Hak Akses Karyawan	0.4	0.1	0	0.1	0.1
Bencana Alam *(Natural Disasters)*	0.29	0.5	0.5	0.5	0.5
Pencurian atau penghancuran aset TI	0.24	1	1	1	1
Pihak luar yang berhasil akses ke sistem	0.08	0.7	0.5	0.7	0.7
Penghentian proses tanpa bencana	0.06	0.2	0.2	0.2	0.2
Kebakaran *(Fire)*	0.01	0.5	0.5	0.5	0.5

Sumber : Kalkulasi Nilai hasil penelitian, diolah kembali

Tabel 8. Kalkulasi Nilai Koefisien Dampak dalam Nilai Finansial (Rupiah)

ISSN (2540-9700)

Tipe Aset TI	Desktop	Monitor	*Mobile Device*	Laptop
Kehilangan Daya (*Power loss*)	Rp 875,063,800	Rp 142,100,400	Rp 894,914,800	Rp 1,846,416,00
Kehilangan Komunikasi	Rp 875,063,800	Rp -	Rp 894,914,800	Rp 1,846,416,00
Kesalahan tidak disengaja	Rp 1,575,114,840	Rp 255,780,720	Rp 1,610,846,640	Rp 3,323,548,80
Virus Komputer	Rp 1,487,608,460	Rp -	Rp 1,521,355,160	Rp 3,138,907,20
Penyalahgunaan Hak Akses oleh Karyawan	Rp 175,012,760	Rp -	Rp 178,982,960	Rp 369,283,20
Bencana Alam (*Natural Disasters*)	Rp 634,421,255	Rp 103,022,790	Rp 648,813,230	Rp 1,338,651,60
Pencurian atau penghancuran aset TI	Rp 1,050,076,560	Rp 170,520,480	Rp 1,073,897,760	Rp 2,215,699,20
Pihak luar yang berhasil akses ke	Rp 245,017,864	Rp 28,420,080	Rp 250,576,144	Rp 516,996,48
Penghentian proses tanpa bencana	Rp 52,503,828	Rp 8,526,024	Rp 53,694,888	Rp 110,784,96
Kebakaran (*Fire*)	Rp 21,876,595	Rp 3,552,510	Rp 22,372,870	Rp 46,160,40

Sumber : Kalkulasi Nilai hasil penelitian, diolah kembali

Untuk mendapatkan jenis aset TI mana yang patut untuk mendapatkan pengendalian, dilakukan *Analysis Across Asset*. Caranya dengan menjumlahkan dan meranking nilai dampak SLE masing-masing aset TI untuk semua *threat* dari tahapan kalkulasi yang terdapat pada Tabel 8 menjadi referensi penentuan ranking jenis aset TI berdasarkan pengurutan dari terbesar hingga terkecil dari nilai dampak SLE dalam nilai Finansial (Rupiah) pada Tabel 9.

Tabel 9 memperlihatkan bahwa aset TI jenis Laptop yang mempunyai nilai dampak kerugian tertinggi jika semua *threat*/risiko terjadi hampir sebesar 15 Milliar rupiah dan aset TI berjenis Monitor yang mempunyai nilai dampak kerugian terendah pada *threat*/risiko yang terjadi. Dengan adanya *Analysis Across Asset* dapat memperlihatkan aset TI mana yang seharusnya dapat diberikan prioritas pengendalian terlebih dahulu dari semua threat/risiko yang terjadi.

Tabel 9. Ranking dan Nilai *Across Asset*

Jenis Aset TI	Nilai *Across Asset* (Rupiah)
Laptop	14,752,863,840
Mobil Device	7,150,369,252
Desktop	6,991,759,762
Monitor	711,923,004
Total	**29,606,915,858**

Sumber : Kalkulasi Nilai hasil penelitian, diolah kembali.

Untuk mendapatkan jenis *threat*/risiko mana yang patut untuk mendapatkan pengendalian adalah dengan melakukan *Analysis Across Risk* dengan menjumlahkan dan meranking nilai dampak SLE (*Single Loss Expectancy*) masing-masing *threat* untuk semua aset TI dari tahapan kalkulasi yang terdapat pada Tabel 8 menjadi referensi penentuan ranking jenis *threat*/risiko berdasarkan pengurutan dari terbesar hingga terkecil dari nilai dampak SLE dalam nilai finansial (Rupiah) pada Tabel 10 Tabel Rangking dan Nilai *Across Risk*.

Tabel 10. Tabel Rangking dan Nilai *Across Risk*

No	Jenis *Risk / Threat*	Nilai Across Aset TI
1	Kesalahan tidak disengaja *(Accidental Errors)*	Rp 6,765,291,000
2	Virus Komputer	Rp 6,147,870,820
3	Pencurian atau penghancuran aset TI	Rp 4,510,194,000
4	Kerugian Daya *(Power loss)*	Rp 3,758,495,000
5	Kerugian Komunikasi *(Communication Loss)*	Rp 3,616,394,600
6	Bencana Alam *(Natural Disasters)*	Rp 2,724,908,875
7	Pihak luar yang berhasil akses ke sistem	Rp 1,041,010,568
8	Penyalahgunaan Hak Akses oleh Karyawan	Rp 723,278,920
9	Penghentian proses tanpa bencana *(Non-disaster downtime)*	Rp 225,509,700
10	Kebakaran (*Fire*)	Rp 93,962,375
	Total	Rp 29,606,915,858

Sumber : Kalkulasi Nilai hasil penelitian, diolah kembali.

Tabel 10 menampilkan nilai dampak finansial yang disebabkan oleh *threat*/risiko hampir sebesar 30 Miliar rupiah untuk aset TI perusahaan dengan jenis *threat* Kesalahan tidak disengaja (*Accidental Errors*) yang mempunyai nilai dampak kerugian tertinggi, hampir mencapai 7 Miliar rupiah untuk semua jenis aset TI. Sedangkan untuk jenis *threat* Kebakaran (*Fire*) mempunyai nilai dampak kerugian terendah untuk aset TI, karena nilai kemungkinan terjadinya *threat* kebakaran hanya 0.01 dalam 1 tahun.

Hasil analisa menunjukkan bahwa aspek aset TI jenis Laptop yang mempunyai potensi nilai kerugian terbesar bagi perusahaan sebesar Rp. 14,752,863,840 untuk semua *threat*/risiko yang terjadi pada aset TI dan aspek *threat*/risiko Kesalahan tidak disengaja (*Accidental Errors*) yang mempunyai potensi nilai kerugian terbesar bagi perusahaan sebesar Rp. 6,765,291,000 untuk semua jenis aset TI.

Hasil analisa tersebut menghasilkan rekomendasi untuk pemangku keputusan yaitu Departement IS Service Management dalam melakukan tindakan pengendalian risiko untuk aspek aset TI jenis Laptop yang mempunyai potensi nilai kerugian terbesar dibandingkan dengan jenis aset TI yang lain dan segera memberikan tindakan pengendalian risiko untuk aspek threat/risiko kesalahan tidak disengaja (*Accidental Errors*) yang mempunyai potensi nilai kerugian terbesar dibandingkan jenis ancaman/risiko yang lain.

SIMPULAN

Penelitian Analisa Manajemen Risiko TI Pemeliharaan aset TI menggunakan QRA dapat mengidentifikasi faktor risiko yang perlu mendapat prioritas pemeliharaan serta jenis aset TI mana saja yang perlu mendapat perhatian khusus dan menghasilkan

rekomendasi jenis aset TI dan faktor risiko yang perlu segera dilakukan analisa pengendalian (*controls*) lanjutan. Untuk melindungi nilai finansial aset TI sebesar Rp. 18,792,475,000 didapatkan kesimpulan bahwa hasil data analisa menunjukkan bahwa aspek aset TI jenis Laptop dengan potensi nilai kerugian sebesar Rp. 14,752,863,840 dan aspek *threat*/risiko kesalahan tidak disengaja (*Accidental Errors*) yang mempunyai potensi nilai kerugian sebesar Rp. 6,765,291,000.

Saran untuk penelitian selanjutnya antara lain melakukan Analisa Pengendalian Risiko (*Analysis Control*) terlebih dahulu dalam menentukan jenis pengendalian (*control*) yang tepat dan akurat untuk mengurangi nilai potensi kerugian pada aspek aset TI jenis Laptop dan aspek threat/risiko kesalahan tidak disengaja (*Accidental Errors*). Selain itu juga dapat dilakukan tindakan Pengendalian Risiko sesuai dengan analisa pengendalian (*control*) untuk aspek aset TI jenis Laptop dan aspek threat/risiko kesalahan tidak disengaja (*Accidental Errors*).

DAFTAR PUSTAKA

Anthony, Rully. 2008. "Mengenal perbankan Indonesia". Diperoleh dari http://hukum-perbankan.blogspot.com. [Accessed: 25-02-2016].

Merrit, J. W. 2000. "*A Method for Quantitative Risk Analysis"*. CISSP. Wang Global. Virginia. Diperoleh dari http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf. [Accessed: 18-03-2016].

Peltier, T. R. 2001. "*Information Security Risk Analysis"* 2nd edition., USA : CRC Press. Boca Raton. Florida. United States. Diperoleh dari http://antoanthongtin.vn/Portals/0/UploadImages/kiennt2/Sach/Sach-CSDL4/Information%20Security%20Risk%20Analysis,%202%20Ed..pdf. [Accessed: 20-03-2016].

Tan, Ding. 2002. "*Quantitative Risk Analysis Step-By-Step*", SANS Institute 2003. Diperoleh dari https://www.sans.org/reading-room/whitepapers/auditing/quantitative-risk-analysis-step-by-step-849. [Accessed: 24-03-2016].