ANALISIS RISIKO PADA SISTEM INFORMASI DI PT. XYZ SEBAGAI BAGIAN PENERAPAN DRP

Yulhendri
Fakultas Ilmu Komputer, Universitas Esa Unggul
Jl. Arjuna Utara No. 9, Kebon Jeruk, Jakarta, 11510
yulhendri@esaunggul.ac.id

Abstract

The business and banking industry tend to develop increasingly complex from time to time, both in terms of business processes that occur, the prevailing organizational structure, to the size of the data and the number of personnel involved in it. Likewise with the role of elements of technology in supporting business operations that are getting bigger and bigger. Information systems, telecommunications networks, and databases for example, have become an inseparable part of the continuity of the operation of a business entity. But not only that, the threat that has the potential to disrupt the functioning of the technology supporting elements of this business is increasingly varied along with the times. These threats include burglary network security, lack of power, employee strikes, and more. Because of its considerable role, the threat to this technological element can be said to be a threat to the sustainability of the company as well. In this paper we discuss how risk analysis contributes greatly to the process of planning and managing DRP. Where do we know DRP is part of BCP. The Risk Analysis process is carried out with a technical analysis of risks related to hardware, lack of power, and human factors. While the development stage of the DRP includes Risk Assessment, Priority Assessment, Recovery Selection and Plant Documenting.

Keywords: *Risk analysis, DRP, risk assestement*

Abstrak

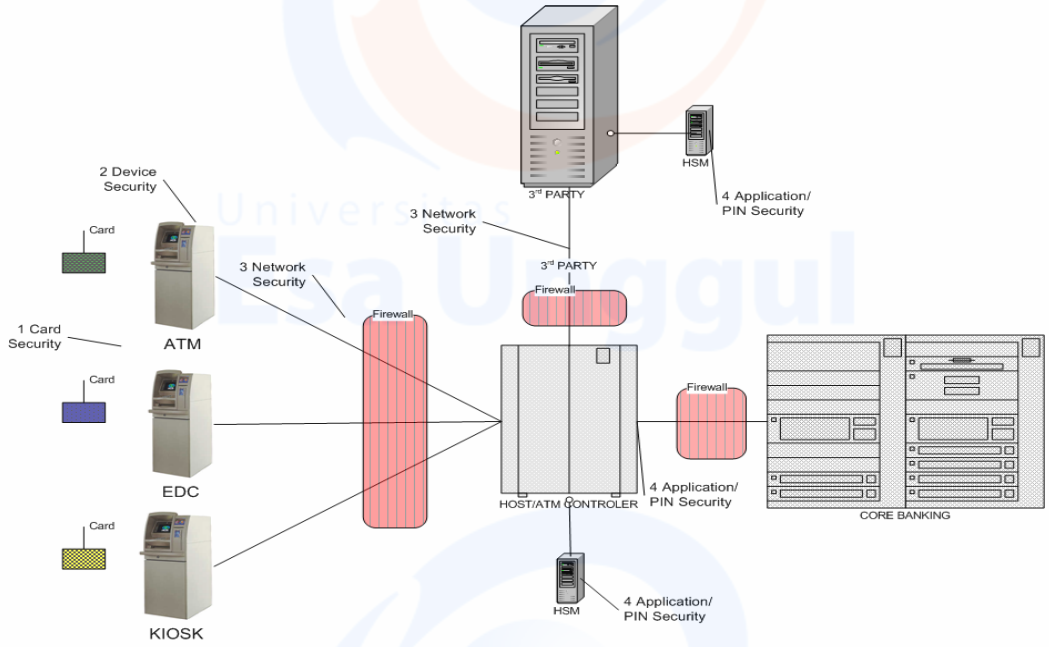
Bisnis dan industri perbankan cenderung berkembang semakin kompleks dari masa ke masa, baik dari segi proses bisnis yang terjadi, struktur organisasi yang berlaku, hingga ukuran data dan jumlah personel yang terlibat di dalamnya. Begitu juga dengan peranan unsur teknologi dalam mendukung operasi bisnis yang semakin lama semakin besar. Sistem informasi, jaringan telekomunikasi, dan basis data misalnya, sudah menjadi bagian yang tidak dapat dipisahkan dari suatu kelangsungan operasi suatu badan bisnis. Namun tidak hanya itu, ancaman yang berpotensi menganggu berfungsinya unsur-unsur teknologi pendukung bisnis ini pun semakin bervariasi seiring dengan perkembangan zaman. Ancaman-ancaman ini antara lain mencakup pembobolan keamanan jaringan, ketiadaan daya, pemogokan pegawai, dan banyak lagi. Karena perannya yang cukup besar, ancaman bagi unsur teknologi ini dapat dikatakan merupakan ancaman bagi keberlangsungan perusahaan juga. Pada tulisan ini dibahas bagaimana analisis risiko berkontribusi besar dalam proses perencanaan dan pengelolaan DRP. Dimana kita ketahui DRP merupakan bagian dari BCP. Proses Analisis Risiko dilakukan dengan analisis risiko dari sisi teknis yang terkait dengan perangkat keras, ketiadaan daya, dan faktor manusia. Sedangkan tahap pengembangan DRP meliputi *Risk Assesstment, Priotity Assesstment, Recovery Selection dan Plant Documenting.*

Kata kunci*:* Analisis risiko*, DRP, risk assestement*

Pendahuluan

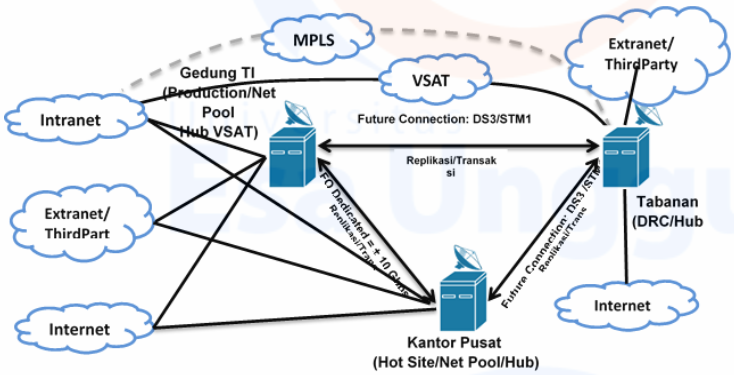
PT. XYZ dalam menjalankan kegiatan operasionalnya, membagi tanggung jawab ke dalam badan kerja-badan kerja. Masing-masing badan kerja tersebut memiliki sistem informasi untuk membantu mereka dalam melakukan fungsinya. Dalam menjalankan fungsi dan tanggung jawabnya masing-masing, unit kerja tersebut seringkali membutuhkan data atau informasi yang dimiliki oleh unit kerja lainnya. Karena itu, pertukaran data antar sistem informasi badan kerja tidak dapat dihindari. Sistem Informasi PT. XYZ adalah sebuah sistem informasi yang dirancang dengan tujuan utama untuk memfasilitasi kebutuhan data antar badan kerja di PT. XYZ..Sistem Informasi PT.

XYZ menyediakan standarisasi data dan pengaturan kewenangan masing masing badan kerja atas data tersebut. Gambar 1 mengilustrasikan Sistem Core Banking di PT. XYZ.



Gambar 1
Sistem Core Banking PT. XYZ

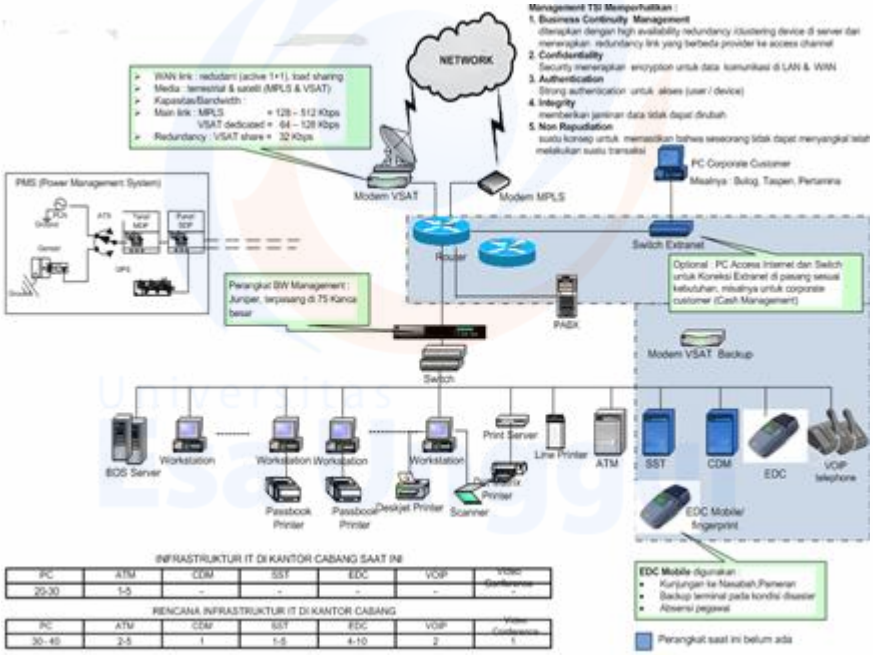
Koneksi jaringan di PT. XYZ secara umum ada 2 yaitu melalui VSAT dan MPLS



Sumber : Data PT. XYZ (2017)

Gambar 2
Koneksi Jaringan di PT. XYZ

Koneksi jaringan dikaitkan dengan rancangan Disaster Recovery Planning (DRP) di PT. XYZ menggunakan beberapa Hub dari kantor pusat ke kantor-kantor cabang dan Hub Ekstranet (*Third Party*).

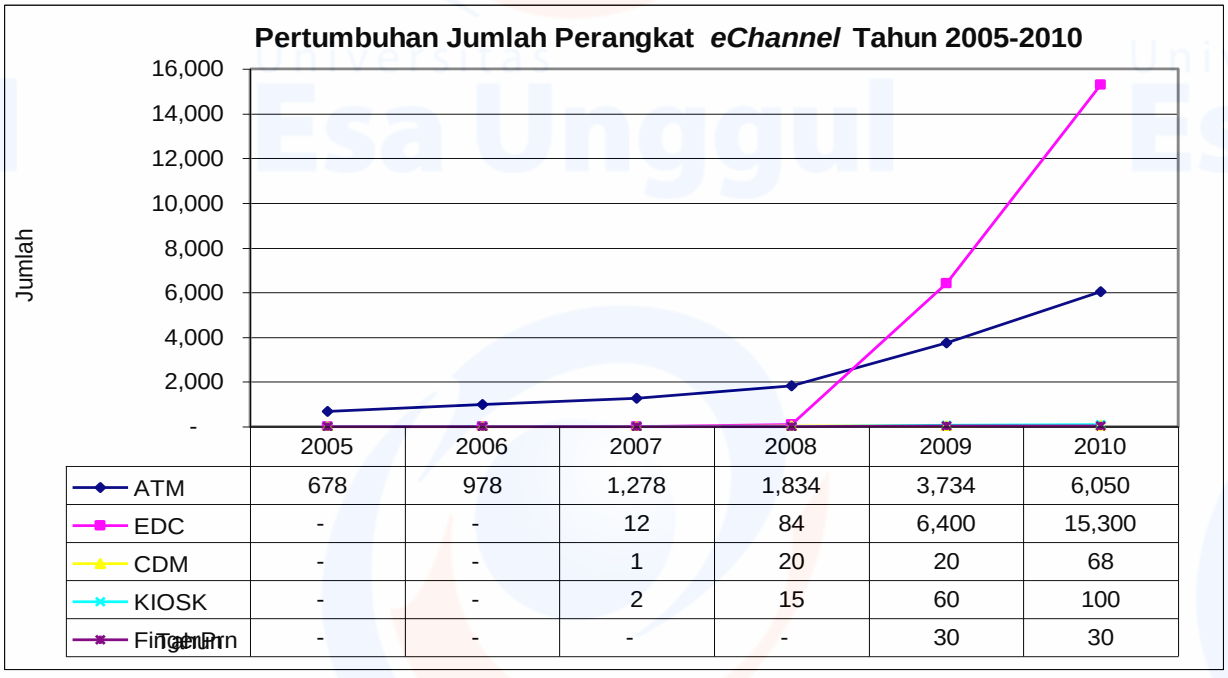


Sumber : Data PT. XYZ (2017)

Gambar 3
Konfigurasi Intranet Kantor Cabang PT. XYZ

Gambar 3 menjelaskan tentang konfigurasi akses kanal intranet di kantor cabang PT. XYZ terhubung ke kantor pusat melalui modem VSAT dan modem MPLS sebagai jalur cadangan. Sementara ke masing-masing perangkat melalui switch dan bandwidth management.

Gambar 4 Menjelaskan konfigurasi akses kanal Intranet di kantor Cabang PT. XYZ yang terhubung dengan seluruh perangkat-perangkat yang ada. Perangkat-perangkat yang ada di kantor cabang antara lain terdiri dari : ATM, EDC, CDM, KIOSK, Finger Print. Dimana jumlah pertumbuhannya dapat dilihat pada gambar 5. (mulai dari tahun 2005 sampai tahun 2010).



	2005	2006	2007	2008	2009	2010
ATM	678	978	1,278	1,834	3,734	6,050
EDC	-	-	12	84	6,400	15,300
CDM	-	-	1	20	20	68
KIOSK	-	-	2	15	60	100
Finger Prn	-	-	-	-	30	30

Sumber : Data PT. XYZ (2017)

Gambar 4.
Pertumbuhan Jumlah Perangkat e-Channel

Analisis Risiko dari Segi Teknis

Seperti yang sudah dijelaskan sebelumnya, Sistem Informasi Manajemen Terintegrasi PT. XYZ merupakan sistem informasi yang melibatkan berbagai macam sistem informasi di PT. XYZ. Sistem informasi-sistem informasi ini dihubungkan dengan menggunakan arsitektur *client/server* berbasis web. *Web service* akan terkoneksi dengan basis data masing-masing sistem informasi melalui jaringan intranet PT. XYZ.

Jaringan intranet yang sama juga menghubungkan antar muka sistem informasi-sistem informasi tersebut dengan pengguna, karena itu ketersediaan jaringan intranet PT. XYZ adalah mutlak untuk Sistem Informasi di PT. XYZ dapat berjalan dengan baik. Analisis risiko dari segi teknis akan berdasar pada hal-hal teknis apa saja yang dapat mengakibatkan terjadinya gangguan pada perangkat keras, perangkat lunak, dan data yang terlibat dalam arsitektur tersebut.

Kerusakan Perangkat Keras

Jaringan intranet PT. XYZ, seperti jaringan intranet pada umumnya, memiliki komponen-komponen seperti *server*, *router*, *switch*, *gateway*, dan lainnya. Agar jaringan dapat berjalan dengan baik, keseluruhan komponen tersebut harus dalam keadaan bekerja. Jika satu atau lebih komponen tersebut tidak tersedia, misalnya karena rusak, kinerja jaringan akan terpengaruh secara langsung. Untuk menghindari kelumpuhan jaringan karena hal semacam ini, umumnya jaringan memiliki lebih dari satu buah untuk masing-masing komponen tersebut. *Router* misalnya, PT. XYZ memiliki dua buah router utama yang berfungsi sebagai simpul-simpul jaringan. Kedua *router* ini diletakkan di tempat yang berbeda-beda untuk menghindari kelumpuhan secara bersamaan.

Kerusakan perangkat keras adalah salah satu gangguan teknis yang paling umum terjadi, karena itu hal ini perlu untuk diperhatikan. Waktu kelumpuhan dapat ditekan jika saat terjadi gangguan, sudah dimiliki nomor atau alamat kontak personel yang dapat memperbaikinya, supplier yang dapat menyediakan alat yang sesuai dengan cepat dan terjamin ketersediaannya, dan lain sebagainya yang termasuk dalam *Disaster Recovery Plan.*

Ketiadaan Daya

Bagaimanapun juga, kelumpuhan tidak dapat dihindari dalam beberapa kasus. Ketiadaan daya misalnya, akan melumpuhkan jaringan secara total. Hal ini tentunya mengakibatkan Sistem Informasi di PT. XYZ tidak dapat menjalankan fungsinya. Ketiadaan daya dapat diakibatkan oleh berbagai macam hal, namun yang paling umum adalah oleh pemadaman listrik dari pihak PLN. Kota Bandung sendiri tercatat cukup sering mengalami pemadaman listrik, puncaknya adalah pada bulan Mei sampai Juli tahun 2017 sebanyak 112 kali di berbagai daerah yang berbeda (berdasarkan hasil survey JCC).

Kerusakan Perangkat Lunak dan Data

Perangkat lunak di sini mengacu pada masing-masing sistem informasi yang menyusun Sistem Informasi PT. XYZ. Termasuk di dalamnya tampilan antar muka, modul-modul pengolah data, dan modul-modul koneksi. Tidak seperti perangkat keras yang dapat diperbaiki ataupun digantikan dengan perangkat yang baru dengan cepat jika rusak, perangkat lunak memiliki proses perbaikan dan instalasi yang cukup memakan waktu dan relatif lebih rumit.

Kerusakan perangkat lunak sangat mungkin terjadi, misalnya saat dilakukan *upgrade* dari satu versi ke versi yang lebih baru, umumnya dengan tujuan menyesuaikan sistem informasi dengan perubahan yang terjadi di dunia nyata, meningkatkan performa, mengganti tampilan dengan yang lebih baik, dan lain sebagainya. Instalasi perangkat lunak baru, baik seluruhnya maupun modular, tidak akan pernah lepas dari proses *debug* dan penyesuaiaan dengan modul-modul lain.

Walaupun umumnya perbaikan tidak dilakukan langsung pada server, melainkan pada repository sementara dulu, dan baru kemudian dipindahkan ke server setelah melalui serangkaian tes, namun tetap tidak menutup kemungkinan terdapat *bug* yang baru ditemukan kemudian. Pada

fase inilah, perangkat lunak menjadi rentan akan kesalahan operasi. Kesalahan pada perangkat lunak juga dapat mempengaruhi data yang tersimpan, dan mengakibatkan kerusakan data.

Faktor Manusia

Selain hal-hal yang telah dijabarkan di atas, masih terdapat faktor kesalahan manusia yang dapat mengganggu operasional PT. XYZ. Misalnya kesalahan pada saat melakukan konfigurasi *server*, tidak sengaja merestart *router*, dan hal-hal lain yang mungkin tidak diperhitungkan sebelumnya. Demikian juga dengan factor keamanan jaringan. Selalu terdapat kemungkinan akan adanya serangan dari luar, seperti *defacing*, manipulasi (menghapus, menambahkan, maupun mengubah) data, pengalihan rute jaringan, dan berbagai macam jenis serangan lainnya. Tidak hanya serangan melalui jaringan, serangan langsung sepeti pencurian ataupun perusakan alat juga bukan hal yang baru lagi. Karena itu, faktor manusia layak diperhitungkan sebagai potensi gangguan.

Hasil Analisis

Dari penjabaran di atas, dapat disimpulkan bahwa terdapat banyak ancaman yang dapat berubah menjadi gangguan bagi Sistem Informasi PT. XYZ. Selain itu, dapat diketahui bahwa PT. XYZ memiliki tingkat ketergantungan yang cukup besar terhadap Sistem Informasi PT. XYZ, terutama pada waktu-waktu tertentu. dengan berbagai macam ancaman yang dapat berubah menjadi gangguan kapan saja. Mempertimbangkan dua hal di atas, disimpulkan bahwa PT. XYZ membutuhkan sebuah *Disaster Recovery Plan* untuk Sistem Informasi PT. XYZ. Dengan *Disaster Recovery Plan* yang baik, jika suatu gangguan bencana terjadi, Sistem Informasi PT. XYZ dapat kembali beroperasi secepat mungkin sehingga PT. XYZ hanya akan mengalami kehilangan/ kerugian minimal. Berikut ini adalah beberapa kebutuhan yang ingin dipenuhi dengan *Disaster Recovery Plan* yang akan dibangun:

1. *Disaster Recovery Plan* akan menangani paling tidak ancaman-ancaman bencana yang sudah dijabarkan pada analisis resiko.
2. *Disaster Recovery Plan* yang *cost effective*, sedapat mungkin menggunakan apa yang sudah dimiliki oleh PT. XYZ (untuk tempat, teknologi, tenaga manusia, dan aset lain yang mungkin dibutuhkan).
3. *Disaster Recovery Plan* yang akan dibangun harus didokumentasikan dengan baik dan mudah dipahami. *Disaster Recovery Plan* harus mudah diperbaharui/ disesuaikan jika terjadi perubahan pada Sistem Informasi PT. XYZ.

Tahap Pengembangan DRP

Tahapan pembangunan sebuah *Disaster Recovery Plan* tidak selalu sama, karena sangat bergantung pada kebutuhan dan tujuan pembuatannya. Dalam pembangunan *Disaster Recovery Plan* untuk Sistem Informasi PT. XYZ, tahapan yang akan dilakukan adalah sebagai berikut:

1. *Risk assessment*

   Merupakan tahap identifikasi ancaman-ancaman yang mungkin terjadi, baik yang berasal dari dalam, maupun dari luar. Bencana yang dianalisa antara lain adalah bencana alam, bencana kegagalan teknis, maupun ancaman-ancaman faktor manusia. Pengukuran akan dilakukan secara kualitatif dengan pendekatan *scoring*.
2. *Priority assessment*

   Tahap dilakukannya pembobotan setiap elemen dari berbagai aspek berdasarkan skala prioritasnya sebagai pendukung sistem. Aspek yang akan ditinjau adalah aspek arsitektur, proses, dan lokasi. Pengukuran prioritas juga akan dilakukan dengan metode *scoring* secara kualitatif.
3. *Recovery strategy selection*

   Hasil yang didapatkan dari tahap *risk assessment dan priority assessment* kemudian akan digunakan sebagai masukan untuk menentukan strategi pemulihan seperti apa yang sebaiknya disusun. Strategi pemulihan akan mencakup isu seperti lokasi cadangan dan metode pemulihan yang akan dilakukan.

4. *Plan documenting*

Tahap penyusunan dokumen *Disaster Recovery Plan*, dimana setiap hasil yang didapatkan dari tahapan-tahapan sebelumnya dituangkan dalam suatu dokumentasi yang terstruktur. Dengan dokumentasi yang baik, diharapkan dapat lebih mudah dan cepat untuk melakukan langkah yang perlu diambil saat terjadi ancaman.

Risk Assessment

Tahap pertama dari pembangunan *Disaster Recovery Plan* adalah *Risk Assessment*. Pada tahap awal ini, bencana-bencana yang sudah dianalisis akan ditentukan nilai ancamnya terhadap Sistem Informasi PT. XYZ. Setiap bencana memiliki atribut-atribut yang dapat diboboti untuk menentukan nilai ancam, atribut bencana yang akan digunakan dalam pembahasan ini adalah *Likelihood, Restoration Time, Predictability. Likelihood* merupakan nilai kekerapan terjadinya ancaman bencana tersebut dalam suatu kurun waktu yang terukur. Nilai *Likelihood* harus nyata, yaitu merupakan hasil dari yang sudah terjadi (*record*) dan bukan merupakan ramalan (*prediction*). *Restoration Time* merupakan nilai panjangnya jangka waktu yang dibutuhkan oleh sistem untuk kembali pulih (beroperasi kembali) jika suatu gangguan terjadi.

Nilai *Restoration Time* dapat berasal dari hasil observasi yang sudah pernah terjadi (*record*) atau berdasarkan standar operasional yang disepakati (contohnya, terdapat kontrak dengan pemasok mengenai jangka waktu dari pemesanan ke penyediaan alat, dan lain sebagainya). *Predictability* merupakan nilai dapat diprediksi atau tidaknya suatu bencana. Hal ini penting karena semakin panjang jangka waktu suatu bencana dapat diprediksi, semakin banyak tindakan yang dapat dilakukan untuk menghindarinya, sehingga semakin sedikit kerusakan/ kerugian yang diderita. Nilai *Predictability* tidak dapat ditentukan dengan skala kuantitatif karena tidak memiliki nilai ukuran yang pasti. Pembobotan nilai *Likelihood, Restoration Time,* dan *Predictability* dalam analisis ini dilakukan dengan metode wawancara, studi dokumentasi, dan observasi. Pembobotan atribut bencana berdasarkan wawancara, observasi, dan studi dokumentasi yang sudah dilakukan dapat dilihat pada Tabel 1 di bawah ini.

Tabel 1
Atribut Ancaman Bencana

No.	Ancaman	*Likelihood* 0-10*	*Restoration Time* 0-10*	*Predictibility* 0-3*	*Score*
1.	Kerusakan Alat	4	5	3	60
2.	Ketiadaan Daya	6	5	2	60
3.	Kerusakan Perangkat Lunak/Data	4	5	1	20
4.	Kesalahan Manusia	5	3	3	45
5.	Serangan jaringan/data	1	3	3	9
6.	Pencurian/perusakan alat	3	5	3	45
7.	Kerusakan gedung	3	5	2	30
8.	Banjir	1	6	2	12
9.	Gempa (Ringan)	4	2	1	8
10.	Gempa (Besar)	1	7	1	7
11.	Gunung Meletus	1	6	2	12
12.	Kebakaran	1	6	3	18
13.	Bencana Sosial	1	5	2	10

Keterangan

1. *Likelihood* (0-10), nilai yang semakin tinggi pada kolom ini menunjukkan bahwa ancaman tersebut semakin tinggi kemungkinan terjadinya
2. *Restoration time* (0-10), nilai yang semakin tinggi pada kolom ini menunjukkan semakin lamanya waktu yang dibutuhkan untuk mengembalikan sistem beroperasi lagi seperti semula setelah gangguan terjadi
3. *Predictability* (0-3), nilai yang semakin tinggi pada kolom ini menunjukkan semakin sulitnya memprediksi datangnya bencana tersebut, sehingga semakin sedikit waktu dan usaha yang dapat dialokasikan untuk menghindari kerugian karenanya.

4. *Score*, merupakan hasil perkalian dari nilai pada kolom-kolom yang berada di sebelah kirinya, nilai pada kolom ini merepresentasikan skala ancaman bencana tersebut terhadap Sistem Informasi PT. XYZ. Rician keterangan nilai pada Tabel 1 dapat dilihat pada Tabel 2.

Tabel 2
Skala Ancaman Bencana

Nilai	*Likelihood*	*Restoration Time*	*Predictibility*
0	Tidak mungkin terjadi	Tidak ada	Dapat diprediksi dengan pasti bahkan sebelum bencana terjadi
1	Terjadi > 5 tahun sekali	1-4 menit	Prediksi dapat dilakukan sebelum bencana terjadi. Namun dengan tingkat kepercayaan yang lemah.
2	Terjadi 2- 5 tahun sekali	5 menit - 1 jam	Prediksi hanya dapat dilakukan setelah terjadi tanda-tanda awal bencana
3	Terjadi 1 - 2 tahun sekali	1 - 6 jam	Tidak dapat diprediksi
4	Terjadi 6 - 12 bulan sekali	6 - 12 jam	-
5	Terjadi 2 - 6 bulan sekali	12 - 24 jam	-
6	Terjadi 1 - 2 bulan sekali	1 - 4 hari	-
7	Terjadi 2 - 4 minggu sekali	5 - 9 hari	-
8	Terjadi 1 - 2 minggu sekali	10 - 14 hari	-
9	Terjadi 1 -7 hari sekali	15 - 30 hari	-
10	Terjadi bebrapa kali dalam 24 jam	Mmembutuhkan waktu > 1 bulan	-

Dengan melihat hasil penilaian pada Tabel 3, dapat disimpulkan bencana mana yang memiliki tingkat ancaman tinggi sehingga patut diwaspadai, dan manayang dapat diletakkan di prioritas yang lebih rendah. Untuk mempermudah, di bawah ini adalah daftar bencana terurut sesuai dengan tingkat ancaman yang dimilikinya.

Tabel 3
Bencana Terurut Tingkat Acaman

No.	Ancaman	*Likelihood* *0-10*	*Restoration Time* *0-10*	*Predictibility* *0-3*	*Score*
1.	Kerusakan Alat	4	5	3	60
2.	Ketiadaan Daya	6	5	2	60
3.	Pencurian/perusakan alat	3	5	3	45
4.	Kesalahan Manusia	5	3	3	45
5.	Kerusakan gedung	3	5	2	30
6.	Kerusakan Perangkat Lunak/Data	4	5	1	20
7.	Kebakaran	1	6	3	18
8.	Banjir	1	6	2	12
9.	Gunung Meletus	1	6	2	12
10.	Bencana Sosial	1	5	2	10
11.	Serangan jaringan/data	1	3	3	9
12.	Gempa (Ringan)	4	2	1	8
13.	Gempa (Besar)	1	7	1	7

Priority Assessment

Priority Assessment Segi Arsitektur

Dari segi arsitektur, Sistem Informasi PT. XYZ tersusun atas berbagai elemen penyusun, yaitu: perangkat keras, perangkat lunak, jaringan, dan data. Jika suatu bencana terjadi dan mengakibatkan elemen-elemen tersebut terancam, yang manakah yang sebaiknya diutamakan dalam usaha penyelamatan/ pemulihan kembali? Untuk mengetahui urutan prioritas elemen-elemen tersebut, tentunya terdapat beberapa atribut yang harus ditinjau. Atribut-atribut tersebut antara lain: *necessity*, *recoverability*, dan *replaceability*. *Necessity* merupakan derajat seberapa tinggi elemen tersebut diperlukan agar sebuah sistem dapat berfungsi. Jika sistem tetap dapat berfungsi, atau hanya sedikit terganggu dengan ketiadaan suatu elemen, maka elemet tersebut dikatakan memiliki derajat *necessity* yang rendah. Sebaliknya jika kinerja sistem terhenti total, atau tidak dapat

beroperasi karena ketiadaan suatu elemen, maka elemen tersebut dikatakan memiliki derajat *necessity* yang tinggi. Dalam kasus Sistem Informasi PT. XYZ dan keempat elemen arsitektur yang sudah disebutkan di atas yaitu perangkat keras, perangkat lunak, jaringan, dan data, sangatlah jelas bahwa keempat elemen tersebut seluruhnya memiliki derajat *necessity* yang setara, yaitu seluruhnya sangat tinggi.

Tidak mungkin Sistem Informasi PT. XYZ dapat beroperasi jika salah satu dari keempat elemen tersebut tidak ada. Karena hal itu, derajat *necessity* akan diabaikan dalam pembahasan mengenai analisis prioritas segi arsitektur. *Recoverability* merupakan derajat mudah tidaknya suatu elemen diperbaiki jika terjadi kerusakan padanya saat terjadi bencana. Karena pada tabel prioritas nantinya nilai-nilai dari atribut-atribut akan dikalikan untuk mendapatkan bobot prioritas, maka elemen yang dapat dengan mudah diperbaiki dikatakan memiliki derajat *recoverability* yang rendah, sedangkan elemen yang sulit diperbaiki akan mendapatkan nilai *recoverability* yang tinggi (terbalik).

Replaceability merupakan derajat mudah tidaknya menggantikan hal yang rusak tersebut dengan hal yang lain untuk menjalankan fungsi yang sama. Contoh, mudah tidaknya suatu sistem operasi yang rusak digantikan dengan sistem operasi lainnya. Karena pada tabel prioritas nantinya nilai-nilai dari atribut-atribut akan dikalikan untuk mendapatkan bobot prioritas, maka elemen yang dapat dengan mudah digantikan dikatakan memiliki derajat *replaceability* yang rendah, sedangkan elemen yang sulit digantikan akan mendapatkan nilai *replaceability* yang tinggi (terbalik).

Tabel 4
Skala atribut prioritas

Nilai	Necessity	Recoverability	Replaceability
1	Sistem tetap dapat berfungsi sempurna. Walaupun elemen tidak ada	Elemen dapat dengan dengan mudah diperbaiki, tenaga ahli sangat mudah ditemui, dengan waktu perbaikan yang sangat singkat	Elemen dapat digantikan dengan mudah tanpa biaya maupun usaha yang berarti
2	Sistem mengalami hambatan/delay dalam menjalankan fungsinya jika elemen tidak ada	Elemen dapat dengan mudah diperbaiki, tenaga ahli cukup mudah ditemui, namun dengan waktu perbaikan yang berdampak pada sistem	Elemen dpat digantikan dengan yang lain namun tetap membutuhkan biaya dan atau usaha yang cukup besar
3	Sistem hanya dapat menjalankan fungsi-fungsi non vital jika elemen tidak ada	Elemen cukup sulit diperbaiki, tenaga ahli cukup sulit ditemui, dan dengan waktu perbaikan yang dapat mengganggu sistem	Elemen dpat digantikan dengan yang lain dengan biaya dan atau usaha yang besar
4	Sistem hanya dapat menjalankan fungsi-fungsi non vital jika elemen tidak ada	Elemen sangat sulit diperbaiki, tenaga ahli sangat sulit ditemui, dan dengan waktu perbaikan yang sangat panjang	Elemen dpat digantikan dengan yang lain dengan biaya dan atau usaha yang sangat besar
5	Sistem tidak dapat berfungsi sama sekali non vital jika elemen tidak ada	Elemen hamper tidak mungkin untuk diperbaiki	Elemen bersifat unik dan tidak dapat digantikan dengan apapun

Hasil dari *Priority Assessment* segi arsitektur dapat dirangkum dalam bentuk tabel seperti yang dapat dilihat pada Tabel 5.

Tabel 5
Hasil *Priority Assessment* Segi Arsitektur

No.	Elemen	Necessity	Recoverability	Replaceabilty	Priority Value
1.	Perangkat keras	5	3	2	30
2.	Perangkat lunak	5	3	4	60
3.	Jaringan	5	2	4	40
4.	Data	5	5	5	125

Berdasarkan nilai prioritas yang didapatkan pada Tabel 5, dapat diurutkan bahwa prioritas elemen dari segi arsitektur pada Sistem Informasi PT. XYZ adalah sebagai berikut seperti yang tercantum pada tabel 6.

Tabel 6
Prioritas Segi Arsitektur (Terurut)

No.	Elemen	Necessity	Recoverability	Replaceabilty	Priority Value
1.	Data	5	5	5	125
2.	Perangkat lunak	5	3	4	60
3.	Jaringan	5	2	4	40
4.	Perangkat keras	5	3	2	30

Dari prioritas segi arsitektur dapat dilihat bahwa data mendapat nilai prioritas paling tinggi yaitu 125. Diikuti dengan perangkat lunak dengan nilai 60, jaringan dengan nilai 40 dan perangkat keras dengan nilai 30.

Kesimpulan

Berdasarkan analisis risiko yang dilakukan pada Sistem informasi PT. XYZ, ditemukan bahwa Data merupakan prioritas utama dari sisi arsitektur yang harus di *recovery* dengan nilai tingkat prioritasnya adalah 125, diikuti oleh perangkat lunak dengan nilai prioritas sebesar 60, dan jaringan dengan nilai prioritas sebesar 40, serta perangkat keras dengan nilai prioritas 30.

Untuk menentukan prioritas penanganan risiko dilakukan dengan melaksanakan analisis risiko yang diikuti dengan proses risk assessment. Dimana kerusakan alat dan ketiadaan daya skor tertinggi (60).

Risk assessment merupakan proses yang harus dilakukan sebelum mengarah pada rancangan DRP (*Disaster Recovery Planning*). Sehingga DRP yang disusun akan lebih terarah dan tepat sasaran.

Daftar Pustaka

Bodenstein, Cindy. (2014). *Six Benefits of Business Continuity management*.

Bowman. Jr, Ronald H. (2008). *Business Continuity Planning for Data Centers and Systems*. New Jersey: John Wiley & Sons, Inc.

Editor. (2015). *4 Essential Components of A BCP*.

Hiles FBCI, Andrew. 2007. *The Definitive Guide to Business Continuity Management*. New Jersey: John Wiley & Sons, Inc.

http://www.continuitysa.com/six-benefits-of-business-continuity-management/. Diakses tanggal 09 Mei 2017.

http://www.techadvisory.org/2015/05/4-essential- components-of-a-bcp/. Diakses tanggal 08 Mei 2017.

MIR3. (2011). *The Definitive Guide to Business Continuity Planning*.

Snedaker, Susan. (2007). *Business Continuity and Disaster Recovery for IT Professional.* Syngress Publishing, Inc.

SOMAP.org (2006). *Open Information Security Risk Management Handbook*.