ISSN: 2302 -2805

RISK ASSESSMENT DAN *BUSINESS IMPACT ANALYSIS* SEBAGAI DASAR PENYUSUNAN DISASTER RECOVERY PLAN (STUDI KASUS DI STMIK AMIKOM YOGYAKARTA)

Mardhiya Hayaty [1)] , Abidarin Rosidi [2)], M.Rudyanto Arief [3)]
Magister Teknik Informatika STMIK AMIKOM YOGYAKARTA
Jl. Ring Road Utara – Condong Catur- Depok Sleman- Yogyakarta
email : mardhiya_hayati@amikom.ac.id [1)] , abi@amikom.ac.id [2)], rudi@amikom.ac.id [3)]

Abstrak

Bencana bisa datang kapan saja, tidak bisa ditentukan kapan, bagaimana terjadinya, dan berapa lama serta dampak yang ditimbulkan.. Disaster Recovery Plan adalah rencana yang dipersiapkan oleh organisasi dalam menghadapi bencana, prosedur dan langkah apa saja yang harus dilakukan tertera pada dokumen ini, sebagai dasar penyusunan dokumen tersebut, diperlukan beberapa penilaian risk assessment yaitu menganalisa terhadap segala kemungkinan ancaman dan business impact analysis menganalisa dampaknya terhadap kegiatan bisnis disebuah organisasi, penelitian ini dilakukan pada layanan sistem informasi mahasisw baru di STMIK AMIKOM Yogyakarta.Hasil penelitian menunjukkan ada beberapa resiko atau ancaman yang berpengaruh terhadap kegiatan-kegiatan penerimaan mahasiswa baru, serta penentuan nilai RPO dan RTO yang dikehendaki oleh organisasi.

Kata kunci :
Risk Management,Business Impacat Analysis,Disaster, Disaster Recovery Plan.

1. Pendahuluan

Teknologi Informasi (TI) merupakan salah satu faktor yang berperan penting dalam kegiatan perusahaan atau organisasi. Banyak kegiatan operasional didukung oleh layanan Teknologi Informasi (TI). Tak bisa dipungkiri penerapan Teknologi Informasi dalam sebuah organisasi sangat berperan penting dalam kegiatan-kegiatan operasional sebuah organisasi, dapat memperoleh informasi dari sumber data yang ada, membantu dalam mengambil keputusan yang optimal, serta meningkatkan layanan kepada end user, meningkatkan posisi bersaing dalam sebuah organisasi.

Jaman sekarang penerapan teknologi informasi di organisasi merupakan suatu kebutuhan dalam menjalankan roda bisnis organisasi tanpa teknologi informasi proses bisnis sebuah organisasi tidak dapat berfungsi dengan baik, lalu bagaimana jika terjadi sebuah *disaster* atau bencana yang mengakibatkan sebagian atau seluruh proses kegiatan organisasi tidak dapat berfungsi ? Jika organisasi tersebut mengalami hal demikian bisa mengakibatkan kerugian, baik kerugian material maupun immaterial.

STMIK AMIKOM sebagai salah satu organisasi yang mengemban amanah masyarakat untuk menyelenggarakan pendidikan berbasis teknologi informasi tentu saja tidak terlepas dari kewajiban memelihara informasi dan menjaga eksistensi informasi tersebut terhadap berbagai ancaman *disaster* atau bencana,oleh karena itu perlu disusun sebuah dokumen disaster recovery plan yang fungsi utamanya mengatur proses pemulihan terhadap ancaman disaster agar kegiatan organisasi tetap berjalan disaat terjadinya *disaster*, akan tetapi penyusunan DRP tersebut harus didahului oleh beberapa langkah yaitu risk assessment (analisa terhadap segala kemungikinan resiko atau ancaman) serta business impact analysis (analisa dampak yang ditimbulkan terhadap kegiatan organisasi).

2. Tinjauan Pustaka

2.1 Penelitian sebelumnya

Penelitian sebelumnya pernah dilakukan oleh King dan kawan-kawan yang berjudul *Lessons of Disaster Recovery Learned for Information Systems Management in US Higher Education* [4]. Hasil dari penelitian tersebut adalah dampak-dampak disaster yang terjadi di amerika dalam kurun waktu 15 tahun dibeberapa perguruan tinggi disana, hasil tersebut menjadi landasan pentingnya sebuah *plan* dalam menghadapi bahaya *disater*, pada penelitian tersebut pembahasan sangat umum serta tidak dijelaskan tentang *risk assessmen,* Padahl *Risk Assessment* merupakan proses penting dalam menentukan mana ancaman yang kritis mana yang tidak, sebagai dasar dalam penyusunan strategi pemulihan bencana pada dokumen DRP.

2.2 Pengertian Disaster (bencana)

Disaster (bencana) didefinisikan sebagai kejadian yang waktu terjadinya tidak dapat diprediksi dan bersifat sangat merusak [2]

2.3 Risk Assessment

Disaster	Penyebab
Alam	Badai, tornado, kebakaran hutan, gempa, banjir, angin kencang, hawa panas
Manusia	Perang, operasi militer, kekerasan, ancaman bom, ledakan, demo pekerja, kehancuran, pencurian data atau komputer, virus, kelalaian manusia.
Kecelakaan	Kecelakaan pesawat terbang, limbah beracun, dan lain-lain.
Teknikal	Kerusakan perangkat keras atau perangkat lunak, gangguan komunikasi, gangguan servis dan operasioanl gedung, gangguan ketersedian listrik, gannguan perngkat pemadam kebakaran dan lain-lain.

Resiko adalah potensi kerugian atau kerusakan yang muncul akibat suatu kejadian dalam hal ini adalah kejadian bencana. Tujuannya adalah mengidentifikasi resiko yang akan ditimbulkan bila terjadi disaster, menghitung potensi kerugian yang timbul akibat bencana dan mengidentifikasi resiko yang paling sering muncul.

Risk Assessment umumnya mencakup unsur-unsur berikut [3]:

1. Identifikasi ancaman yang bisa merugikan yang akan mempengaruhi proses bisnis yang vital. Ancaman dapat mencakup seperti unsur penyusup, penjahat , teroris, bencana alam dll.
2. Identifkasi tingkat kejadian yang sudah atau yang akan terjadi
3. Estimasi kemungkinan ancaman akan terwujud berdasarkan sejarah informasi, penelitian dan pengetahuan individu.
4. Estimasi terhadap proses paling kritis dan sensitif, potensi kerugian atau kerusakan yang mungkin terjadi jika ancaman terjadi termasuk biaya pemulihan.

Resiko-resiko Quantitative misalnya diperkirakan rata-rata downtime adalah 40 jam per tahun. Biasanya pemberian estimasi ini melibatkan banyak factor. Dan sering mengalami kesulitan dalam memberikan metric resiko ini secara akurat.

Jika pemberian metric Qualitative pada resiko-resiko bisa akurat ditentukan, maka kemungkinan dari suatu resiko yang direalisasikan pada suatu system bisa di set sebagai "1" untuk "Low", "2" untuk criticality "Medium" dan "3" untuk tingkat criticality "High". Bahkan untuk assessment dalam bidang keselamatan perlu menambahkan "Extremely High" dengan angka criticality 4.

Kesulitan yang paling mendasar dalam menentukan tingkat kejadian atau seberapa besar kemungkinannya dari bencana atau tidak berfungsinya sistem aplikasi adalah bila tidak adanya informasi statistik dari kejadian yang telah terjadi dimasa lampau [1].

Setelah kita mendapatkan probability suatu resiko (Low, Medium, High) serta kemungkinan dampak atau impact nya terhadap fungsi bisnis, maka gunakan *matrix risk assessment* untuk menentukan level dari suatu resiko. Berikut adalah matrix risk assessment yang merupakan *Exposure calculation matrix*.

Formulanya adalah Resiko = Probability Ancaman X Dampak Ancaman

Tabel 2.2. *Exposure calculation matrix*

RISK		IMPACT		
		Low(1)	Medium(2)	High(3)
LIKELIHOOD	High(3)	3x1= 3 LOW	3x2= 6 MED	3x3= 9 HIGH
	Medium(2)	2x1= 2 LOW	2x2= 4 MED	2x2= 6 MED
	Low (1)	1x1= 1 LOW	1x2=2 LOW	1x3= 3 LOW

Risk Scale adalah skala resiko dikatakan rendah jika risk scale antara 1-3, medium 4-6 dan high 7-9. Jika skala resiko bernilai "High" bisa diartikan resiko atau ancaman mempunyai resiko tinggi terhadap perusahaan, hal ini berdampak kepada kegiatan bisnis sebuah perusahaan. Hasil pengukuran pada risk assessment dapat berfungsi sebagai kendali-kendali resiko, sehingga perusahaan bisa meningkatkan kontrol-kontrol terhadap kegiatan bisnis yang vital dan pada akhirnya bisa menekan kerugian-kerugian yang mungkin timbul.

2.4 Business Impact Analysis

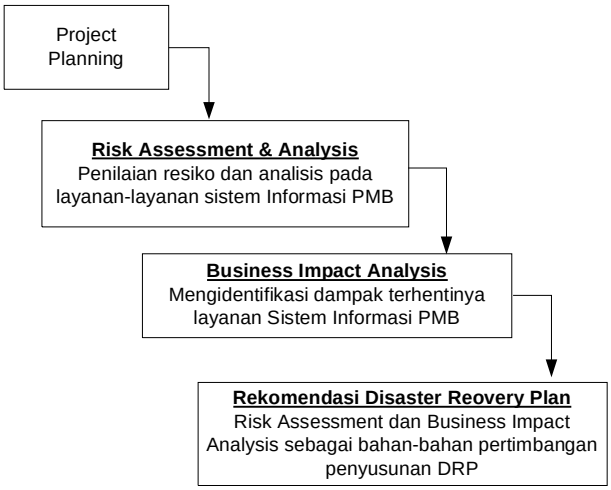
Pengaruh akibat terjadinya sistem tidak berfungsi adalah merupakan hal pokok yang harus dipertimbangkan agar operasional dapat berjalan dengan normal, oleh karena itu dampak-dampak yang terjadi harus dianalisa dengan menggunakan Business Impact Analysis (BIA).

BIA menggunakan informasi yang dihasilkan oleh *risk assessment* yaitu hasil analisa ancaman-ancaman atau resiko yang mungkin akan terjadi, kemudian dihubungkan dengan kegiatan-kegiatan atau proses bisnis yang terjadi diperusahaan, jadi bisa dikatakan jika ancaman tersebut terjadi terhadap kegiatan di perusahaan akan berdampak apa terhadap perusahaan atau kustomer ? Sehingga dengan metode ini dapat ditentukan proses bisnis utama yang sensitif terhadap ancaman disaster.

ISSN: 2302 -2805

BIA juga dimaksudkan untuk membantu organisasi dalam memahami potensi kerugian atau dampak lain yang tidak diharapkan misalnya pada proses operasional dan bisnis yang vital, serta aset-aset teknologi informasi ketika sistem tidak dapat berfungsi maupun dampak non finansial misalnya terhadap pelayanan dan kepuasan pelanggan. Informasi yang dihasilkan oleh aktifitas proses ini diantaranya adalah menentukan periode waktu yang dapat ditolerir oleh sebuah organisasi.

3. Metode Penelitian



Keterangan langka-langkah penelitian pada gambar 3.1 adalah :

1. Project Planning, pada tahapan ini dilakukan pembuatan ruang lingkup masalah yang akan diteliti yaitu layanan-layanan yang berkaitan dengan Sistem Informasi PMB di STMIK AMIKOM.
2. Risk Assessment and Analysis, pada tahap ini dilakukan identifikasi resiko atau ancaman yang akan ditimbulkan, melakukan identifikasi resiko yang paling sering muncul pada layanan-layanan sistem infomasi PMB di STMIK AMIKOM.
3. Business Impact Anlysis, pada tahap ini dilakukan analisa pengaruh atau dampak yang terjadi ketika layanan terhenti, menentukan proses-proses utama yang sensitif terhadap ancaman, dalam tahap ini juga digunakan informasi yang dihasilkan pada tahapan Risk Assessment
4. Hasil analisa Risk assesment dan Business Impact Analysis sebagai dasar usulan yang digunakan untuk merancang DRP.

4. Hasil dan Pembahasan

4.1 Risk Assessment

Pada Risk Assesment dilakukan analisa resiko-resiko yang pernah dan atau mungkin terjadi pada masa implementasi sistem informasi pendaftaran mahasiswa baru. Masa implementasi sistem informasi terjadi antara bulan februari sampai dengan bulan september disetiap tahun akademik penerimaan mahasiswa baru dalam kurun waktu 5 tahun terakhir.

Berdasarkan hasil wawancara dan dukungan data yang terkait, terdapat enam resiko atau ancaman yang beresiko tinggi yang akan berpengaruh terhadap sistem informasi mahasiswa baru, yaitu :

1. Tidak ada supply listrik dari supllier listrik, contoh PLN
2. Supply listrik alternatif (genset) tidak berfungsi
3. Tidak tersedianya service internet dari ISP (internet service provider)
4. Kesalahan pemasangan perangkat.
5. Kesalahan seting/konfigurasi jaringan
6. Perubahan kebijakan dari lembaga sehingga mengharuskan aplikasi yang ada harus dirubah

4.2 Business Impact Analysis

Hasil dari penilaian risk assessment secara garis besar adalah adanya resiko atau ancaman ketiadaaan sumber daya listrik, ketiadaan service internet, kesalahan pemasangan dan konfigurasi jaringan serta adanya perubahan kebijakan. Ancaman tersebut berpengaruh terhadap kegiatan-kegiatan yang dilakukan, dalam hal ini kegiatan tersebut adalah proses penerimaan mahasiswa baru melalui sistem informasi yang diimplementasikan.

Tabel dibawah ini adalah kegiatan-kegiatan yang terjadi pada proses penerimaan mahasiswa baru, volume puncak serta waktu terjadinya volume puncak. Data yang disajikan berdasarkan kegiatan PMB selama kurun waktu 5 tahun terakhir.

Tabel 4.2. Penyebaran bulan volume puncak transaksi

NO	KEGIATAN	Feb	Mar	Apr	Mei	Juni	Juli	Agust	Sept
1	Pendaftaran mahasiswa baru					1682			
2	Pengesahan Pendaftaran/Cetak Kartu ujian					1403			
3	Ujian online					516			
4	Pengumuman hasil ujian online					516			
5	Ujian wawancara					703			
6	Pengumuman hasil wwancara					703			
7	Registrasi pembayaran/Cetak Kwitansi sementara							868	
8	Pembayaran melalui gerai muamalat							676	
9	Her-registrasi							799	
10	Cetak foto ktm								883
11	Tutup buku harian dengan Bank Muamalat								1

Analisa lainnya adalah pada bulan Juni-juli adalah bulan terjadinya volume puncak hampir sebagian besar kegiatan PMB yaitu pendaftaran mahasiswa baru, pengesahan kartu pendaftar, ujian online, ujian wawancara, pengumuman hasil ujian. Jika dijumlahkan semua proses tersebut maka dihasilkan 5523 transaksi terjadi selama bulan juni-juli dengan jumlah calon pendaftar kurang lebih sebanyak 1682 orang. Rata-rata setiap jamnya petugas menggunakan sistem untuk melayani sebanyak 25 transaksi (5523 transaksi / 224 jam) atau sehari 125 transaksi. Jika sistem tidak berfungsi pada bulan tersebut maka organisisi akan

memberikan pelayanan yang buruk kepada pendaftar kurang lebih sebanyak 1682 orang dengan jumlah 5523 transaksi. Hal tersebut secara langsung berpengaruh terhadap pencitraan STMIK AMIKOM itu sendiri, calon pendaftar berangggapan selama ini STMIK AMIKOM adalah lembaga yang konsen terhadap kemajuan teknologi informasi, harapannya semua layanan dapat dilayani dengan baik dengan waktu yang singkat.

Pada bulan agustus terjadi volume transaksi pada kegiatan pembayaran mahasiswa dan her-registrasi mahasiswa yaitu sebanyak 2343 transaksi dengan rata - rata perhari 100 transaksi (25 transaksi perjam x 5 jam pelayanan sehari). Pembayaran mahasiswa dilakukan melalui bank yang di tunjuk atau bisa dilakukan melalui bank lain. Pembayaran yang dilakukan melalui bank yang ditunjuk adalah bank yang membuka gerainya di lingkungan STMIK AMIKOM. Sistem pembayaran yang ada pada bank tersebut terintegrasi dengan sistem informasi STMIK AMIKOM, sehingga setiap harinya selalu dilakukan kros cek data keuangan dengan pihak petugas bank. Jika sistem mengalami kegagalan satu hari saja, proses pembayaran menjadi tertunda walaupun bisa ditangani secara manual tetapi tentu saja memerlukan proses yang lebih lama, antrian menjadi lebih panjang apalagi tidak tersedianya jumlah sumber daya manusia yang memadai(petugas).

Data pada tabel 4.2 tentang penyebaran bulan volume puncak transaksi menunjukan nilai *Recovery Point Objective (RPO)* yang mungkin bisa ditolerir STMIK AMIKOM dalam menoleransi kegagalan sistem adalah pada bulan Februari sampai dengan bulan Mei, dan bulan Agustus sampai dengan September untuk proses kegiatan pendaftaran mahasiswa baru, pengesahan kartu pendaftar, ujian online, ujian wawancara, pengumuman hasil ujian karena pada bulan – bulan tersebut volume transaksi dianggap relatif kecil, sedangkan pada bulan Juni sampai dengan Juli nilai yang yang mungkin bisa diberikan adalah 0, artinya pada bulan tersebut sistem diharapkan tidak boleh tidak berfungsi dikarenakan volume transaksi sangat besar di bulan tersebut. Nilai RPO untuk kegiatan pembayaran mahasiswa baru yang mungkin bisa ditolerir adalah pada bulan Februari sampai dengan Juli serta bulan september, sedangkan bulan Agustus nilai RPO adalah 0 karena volume transaksi mengalami puncaknya dibulan tersebut. Sedangkan nilai RPO untuk kroscek data keuangan antara gerai bank dengan STMIK AMIKOM adalah 0 setiap jam 15.000 WIB setiap hari senin-jumat, karena pada jam tersebut dilakukan closing pembukuan.

Jika sebuah ancaman terjadi dan mungkin mengakibatkan kegagalan sistem secara keseluruhan maka perlu adanya waktu yang mengindikasikan seberapa lama infrastruktur teknologi informasi akan dipulihkan. Pihak manajemen mengharapkan nilai Recovery Time Object (RTO) atau sistem akan pulih dalam waktu satu hari pada kegiatan pendaftaran mahasiswa baru, pengesahan kartu pendaftar, ujian online, ujian wawancara, pengumuman hasil ujian. Berdasarkan hasil analisa volume puncak transaksi didapat rata-rata transaksi perhari adalah 125 perhari, maka selama sistem tidak berfungsi selama satu hari akan terjadi gangguan pelayanan sebanyak 125 transaksi. Sedangkan nilai RTO untuk pembayaran adalah satu hari dengan 100 volume transaksi akan terganggu. Nilai RTO yang diberikan untuk kegiatan tutup buku antara bank dengan AMIKOM hanya ditoleransi oleh organisasi sebesar 1 jam, artinya setelah satu jam sistem sistem harus berjalan dengan normal.

5. Kesimpulan dan Saran

5.1 Kesimpulan

1. Terdapat enam resiko atau ancaman yang beresiko tinggi yang akan berpengaruh terhadap sistem informasi mahasiswa baru.
2. Dampak yang terjadi jika resiko atau ancaman tersebut benar-benar terjadi terhadap kegiatan – kegiatan proses penerimaan mahasiswa baru secara keseluruhan adalah terganggunya proses pelayanan terhadap calon serta terganggunya proses klarifikasi data keuangan dengan pihak bank mengingat sistem bank yang membuka kantor kas di AMIKOM terintegrasi langsung dengan sistem informasi AMIKOM.
3. Nilai waktu toleransi (RTO=Recovery Time Object) yang diberikan dalam mentolerir kegagalan sistem oleh STMIK AMIKOM adalah satu hari untuk proses kegiatan pendaftaran mahasiswa baru, pengesahan kartu pendaftar, ujian online, ujian wawancara, pengumuman hasil ujian, pembayaran dan her-registrasi dan satu jam untuk klarifikasi data dengan pihak bank.

5.2 Saran

1. Perlu dibuat sebuah *Disaster Recovery Plan* yang didalamnya memuat prosedur-prosedur pemulihan terhadap kegagalan sistem sebagai akibat yang ditimbulkan oleh bencana atau *disaster* berdasarkan berbagai ancaman (dari hasil *risk assesment*) dan dampak yang akan ditimbulkan (dari hasil *Business Impact Anlysis*).
2. Perlu dilakukan penelitian lebih mendalam seberapa besar dampak terganggunya layanan sistem informasi di AMIKOM terhadap kepuasan pelayanan terhadap calon pendaftar atau masyarakat.
3. Perlu dilakukan penelitian lebih mendalam tentang dampak terganggunya sistem terhadap kondisi keuangan atau pendapatan di STMIK AMIKOM.

Daftar Pustaka

[1] Cahyadi, Eddy, 2006, Kajian Business Continuity Plan Berdasarkan Kuantifikasi Nilai Ekonomis Sistem Aplikasi Pada Industri Penerbangan : Studi kasus pada PT.Garuda Indonesia, Tesis, Magister

ISSN: 2302 -2805

Ilmu Komputer program studi Teknologi Informasi Universitas Indoenesia, Jakarta.

[2] Irham, Dolly, 2008, Kajian Disaster Recovery Center Call Center pada Industri Perbangkan, Tesis, Magister Teknologi Informasi, Universitas Indonesia, Jakarta.

[3] Kefallinos Dionysis, Lambrou Maria A. and Sykas Efstathios D, 2009, *An Extended Risk Assessment Model for Secure E-Government Projects*, International Journal of Electronic Government Research, Vol. 5. - 1548-3886. Vishanth Weerakkody (Brunel University UK).

[4] King Ruben [et al.], june 2010, *Lessons of Disaster Recovery Learned for Information Systems Management in US Higher Education*, International Journal of Information Systems for Crisis Response and Management (IJISCRAM), Vol. 2. - ISSN: 1937-9390.

Biodata Penulis

Mardhiya Hayati, memperoleh gelar Sarjana Teknik (S.T), Fakutas Teknik Program Studi Teknik Informatika Universitas Ahmad dahlan Yogyakarta, lulus tahun 2003.. Saat ini sebagai staf pengajar program Teknik Informatika STMIK AMIKOM Yogyakarta.

M. Rudyanto Arief, memperoleh gelar Magister Teknik (MT), Fakultas Teknik Elektro Universitas Gajah Mada tahun 2005. Saat ini sebagai staf pengajar program Magister Teknik Informatika STMIK AMIKOM Yogyakarta dan sebagai kepala Penjamin Mutu STMIK AMIKOM Yogyakarta.

Abidarin Rosidi, memperoleh gelar Doktor di Universitas brawijaya Malang. sebagai staf pengajar program Magister Teknik Informatika STMIK AMIKOM Yogyakarta dan sebagai direktur Magister Teknik Informatika STMIK AMIKOM Yogyakarta.

ISSN: 2302 -2805