Proceedings

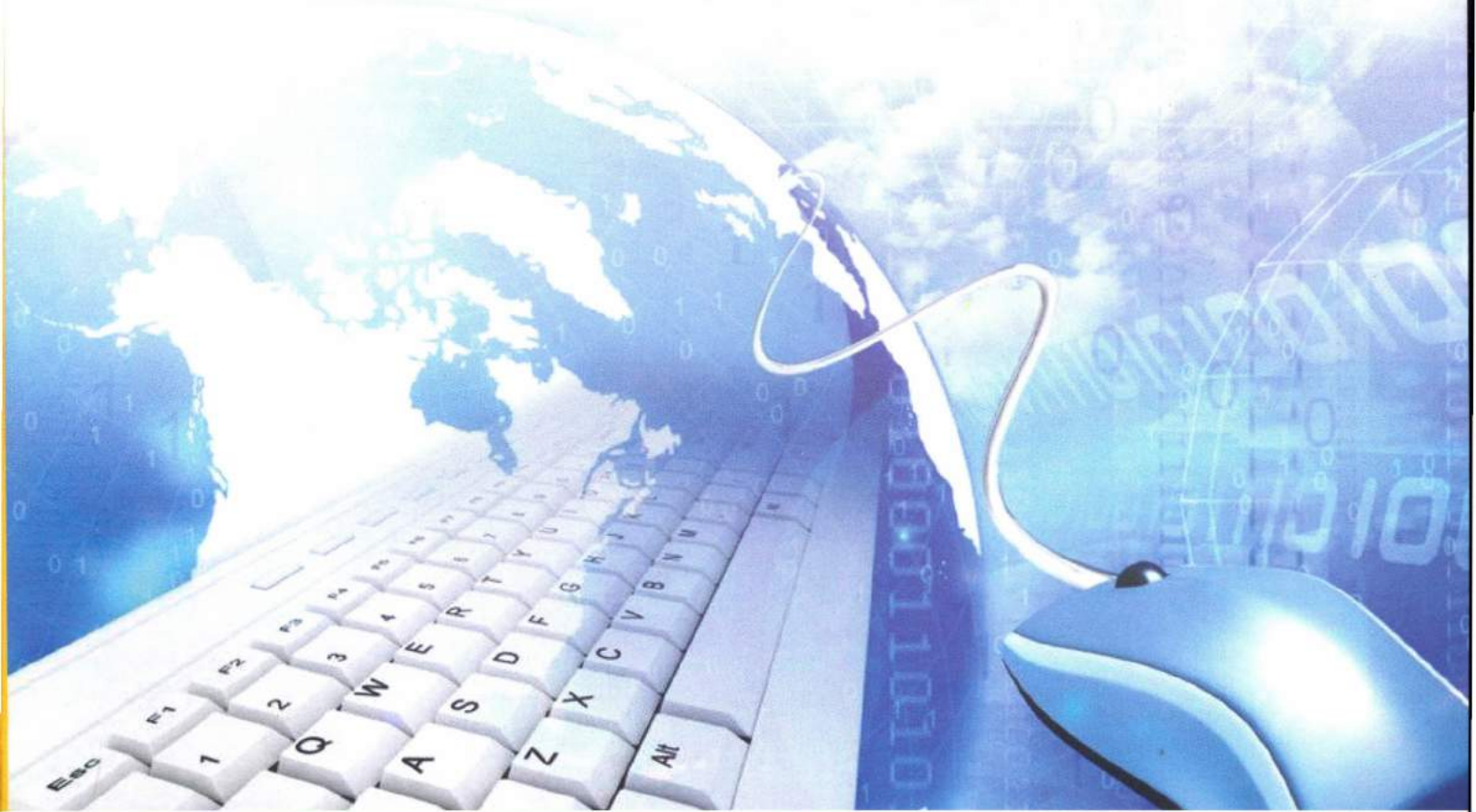
Konferensi Nasional Sistem Informasi 2012

STIKOM BALI
Always The First

23 - 25 Pebruari 2012

Abstract Proceeding Edition

ISBN : 9786029876802



P3M STIKOM Bali
JL. Raya Puputan No. 86 Renon, Denpasar - Bali
Phone : +62-361-244445 | Fax. : +62-361-264773
Email : info@stikom-bali.ac.id

PROCEEDINGS

KONFERENSI NASIONAL SISTEM INFORMASI 2012

KOMITE KNSI 2012

PENANGGUNG JAWAB :
Drs. Dadang Hermawan, Ak.,MM
Ketua Sekolah Tinggi Manajemen Informatika dan Teknik Komputer (STMIK) STIKOM Bali

KETUA KOMITE PELAKSANA KNSI 2012
Evi Triandini, SP.,M.Eng

STEERING COMMITTEE :

Kridanto Surendro, Ph.D
Dr. Rila Mandala, M.Eng
Dr. Ir. Husni S Sastramiharja, MT
Prof. Iping Supriatna
Dr. Ing. M. Sukrisno
Drs. Dadang Hermawan Ak.,MM

PROGRAM COMMITTEE :

Kridanto Surendro, Ph.D (ITB)
Dr. Rila Mandala (ITB)
Dr. Husni Setiawan Sastramihardja (ITB)
Prof. Jazi Eko Istiyanto, Ph.D (UGM)
Prof. Dr. Beny A Mutiara (Univ. Gunadarma)
Retantyo Wardoyo, Ph.D (UGM)
Agus Harjoko, Ph.D (UGM)
Dra. Sri Hartati, M.Sc, Ph.D (UGM)
Zainal A. Hasibuan, Ph.D (Univ. Indonesia)
Dr. Djoko Soetarno (Univ. BINUS)
Prof. Ir. Arief Djunaedi, M.Sc.,PhD (ITS)
Prof. Dr. Ir. Joko Lianto Buliali, MSc (ITS)
Dr. Ir. Agus Buono, M.Si., M.Kom (IPB)
Dr. Ir. Sri Nurdiati, M.Sc (IPB)
Yudi Agusta, PhD (STIKOM Bali)
Prof. Dr. M. Zarlis, M.Sc (USU)

PANITIA :

I Made Sarjana
Ni Luh Putri Srinadi
IB. Suradarma
Roy Rudolf Huizen
I Ketut Dedy Suryawan
Ni Made Kartini
Ni Wayan Deriani
Luh Dwi Ari Sudawati
Desy Tri Puspasari
Ni Made Kansa Putri
Candra Ahmadi
I Gusti Rai Agung Sugiartha
Shofwan Hanief
Ricky Aurelius N Diaz
I Made Budi Adnyana
I Wayan Kardana
I Gede Harsemadi
Dian Pramana
I Gede Putu Krisna Juliharta
I Gusti Komang Oka M
Dandy Pramana Hostiadi
Ahmad Arfai Syukri
I Gede Mudjana
Zaenal Arifin
I Made Sukerta
Esron Rasi Oematan
Ni Putu Anita Diastuti
Andre Stafiyan
Erma Sulistyo Rini
Ida Ayu Kencana Dewi
Ni Luh Ratniasih
Gusti Agung Vony Purnama,
Dian Permana Yoga
I Gede Muriarka
Tubagus Mahendra Kusuma
I Gusti Ngurah Agung
Dedy Panji Agustino
I Wayan Budiarta
Andri Setyia Raharjo

MODEL MANAJEMEN RISIKO TEKNOLOGI INFORMASI UNTUK KEBERLANJUTAN LAYANAN TEKNOLOGI INFORMASI STUDI KASUS DI PT. XYZ

Irfan Maliki

Jurusan Teknik Informatika
Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonesia (UNIKOM)
Jl. Dipatiukur no 112-116 Bandung 40132, Indonesia, Telp. +622533825
Irfanmaliki007@gmail.com

Abstrak

Fakta semakin meningkatnya ketergantungan perusahaan pada teknologi informasi untuk mencapai tujuan strategi dan kebutuhan perusahaan menjadi pendorong utama pentingnya TI. Ketergantungan tersebut menyebabkan tumbuhnya kebutuhan akan layanan TI berkualitas tinggi yang mengikuti kebutuhan perusahan dan pengguna sesuai dengan perkembangannya. Proses Bisnis perusahaan yang memanfaatkan layanan TI tidak dapat terhindar dari adanya risiko-risiko yang disebabkan oleh kerusakan alam maupun kerusakan yang diakibatkan oleh manusia (internal ataupun eksternal). Kerusakan yang terjadi tidak hanya berdampak pada kemampuan teknologi yang digunakan, tetapi juga berdampak pada layanan operasional sehingga dibutuhkan pengelolaan terhadap risiko-risiko tersebut. Dalam pembangunan model manajemen risiko TI didasarkan pada kerangka kerja yang telah direkomendasikan yang terdiri dari COBIT, dan ISO/IEC 27005. Pembangunan model manajemen risiko TI untuk keberlanjutan layanan TI telah berhasil dilakukan dengan menetapkan sejumlah proses yang dapat dilakukan untuk manajemen risiko TI. Model manajemen risiko TI untuk keberlanjutan layanan TI telah berhasil diuji dan divalidasi dengan menggunakan uji statistik. Metode Pearson, analisis regresi, dan analisis regresi ganda digunakan sebagai metode untuk pengujian. Dari hasil pengujian tersebut dapat ditetapkan bahwa model dapat diterapkan atau diimplementasikan.

Keywords: Manajemen risiko TI, Keberlanjutan layanan TI, Penilaian risiko, Risiko TI.

1. PENDAHULUAN

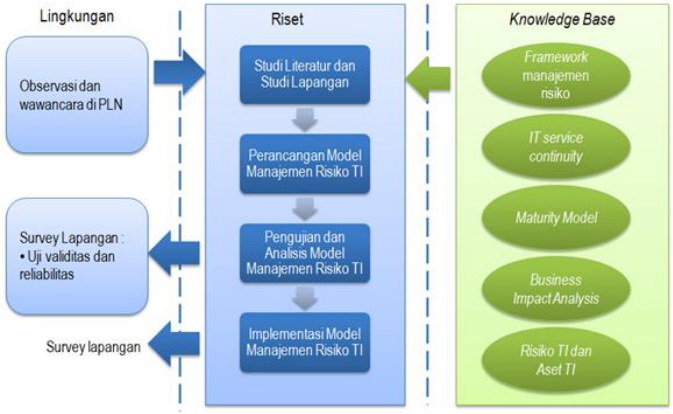
Fakta semakin meningkatnya ketergantungan perusahaan kepada teknologi informasi (TI) untuk mencapai tujuan strategi dan kebutuhan perusahaan menjadi pendorong utama pentingnya layanan TI. Namun layanan TI tersebut tidak dapat terhindar dari adanya risiko TI yang disebabkan oleh kerusakan alam, maupun kerusakan yang diakibatkan oleh manusia. Menurut Priyadi [7] bahwa perusahaan dan para manajernya tidak memiliki cara yang sama dalam menghadapi risiko TI. Kerusakan .yang terjadi tidak hanya berdampak pada kemampuan teknologi yang digunakan, tetapi juga berdampak pada layanan operasional. Bila tidak ditangani secara khusus, selain akan menghadapi risiko operasional, juga akan mempengaruhi risiko reputasi dan berdampak pada menurunnya tingkat kepercayaan *customer*.

Dalam menghadapi setiap kemungkinan ancaman tersebut perlu dilakukan penilaian risiko sehingga dapat memperkirakan adanya ancaman (*threat*), kelemahan (*vulnerability*) serta dapat memutuskan pilihan yang akan diambil, apakah memilih dan mengabaikan suatu ancaman atau memberikan pengurangan terhadap proteksinya. Instalasi ukuran pengendaliannya berdasarkan suatu keseimbangan antara *cost of control* dan kebutuhan untuk mengurangi atau menghilangkan ancaman. Seperti dalam analisis risiko, yang pada dasarnya merupakan suatu pendekatan manajemen risiko, untuk membantu mengidentifikasi ancaman dan memilih kriteria ukuran keamanan yang menghasilkan *cost-effective* [1]. Dengan menerapkan manajemen risiko khususnya pada layanan TI, perusahaan tidak hanya dapat mereduksi adanya *exposure* risiko informasi tetapi juga dapat mengurangi biaya yang harus dikeluarkan dari adanya *exposure* tersebut.

PT. XYZ, sebagai salah satu perusahaan yang memanfaatkan TI untuk mendukung keberlangsungan bisnis, membutuhkan ketersediaan layanan TI yang tinggi. Operasional yang dilaksanakan disetiap bagian organisasi, sangat bergantung pada tersedianya layanan TI sehingga apabila terjadi gangguan atau kerusakan pada layanan tersebut dapat memberikan dampak yang signifikan pada keberlangsungan bisnis perusahaan. Salah satu layanan TI yang dimanfaatkan oleh PT XYZ adalah pengelolaan data pelanggan, dimana saat ini jumlah pelanggan perusahaan mencapai kurang dari 10 juta pelanggan, jika dilihat dari

transaksi data yang dilakukan, baik harian maupun perbulan memiliki tingkat layanan yang begitu tinggi. Apabila data tersebut mengalami kesalahan, kehilangan dan kerusakan data, maka membutuhkan biaya dan *effort* yang besar untuk menanggulanginya. Untuk menghindari hal ini diperlukan sebuah langkah yang nyata dan cepat untuk minimalisasi risiko TI yang terjadi. Bagian TI sebagai pengelola dan penyedia layanan TI, dipandang perlu untuk mengelola risiko TI tersebut agar keberlangsungan bisnis tetap dapat didukung. Saat ini kajian mengenai manajemen risiko untuk layanan TI belum sepenuhnya dilakukan dan diterapkan dilingkungan PT. XYZ. Oleh karena itu dalam penelitian ini diusulkan sebuah model manajemen risiko TI untuk keberlanjutan layanan TI yang diharapkan dapat membantu pihak pengelola layanan TI untuk mengelola risiko TI.

Adapun metodologi penelitian yang dilakukan dalam penelitian ini dapat dilihat pada gambar 1 berikut:



Gambar 1. Metode Penelitian

2. TINJAUAN PUSTAKA

2.1 Manajemen Risiko

Risiko adalah dampak negatif yang diakibatkan dengan adanya kerentanan, berdasarkan dari pertimbangan baik probabilitas maupun dampak kejadian [8]. Selanjutnya Spremic [9] menjelaskan bahwa risiko merupakan fungsi kemungkinan (*likelihood*) sumber ancaman (*threat-source*) mengeksploitasi kerentanan (*vulnerability*) potensial, yang menghasilkan dampak (*impact*) kejadian yang merugikan organisasi. risiko-risiko yang terjadi pada pemanfaatan TI dapat memberikan dampak negatif terhadap aset TI (data, *software, hardware*), layanan-layanan TI, bisnis proses, serta organisasi secara keseluruhan. Oleh sebab itu risiko tersebut perlu dikelola dengan baik [9].

Manajemen risiko TI merupakan proses identifikasi risiko, penilaian risiko, dan pengambilan langkah-langkah untuk menurunkan risiko sampai level yang dapat diterima [8]. Sedangkan menurut IT governance, IT Audit dan IT Security dalam [9], manajemen risiko TI adalah proses untuk memahami dan memberikan respon terhadap faktor-faktor yang dapat menyebakan kegagalan dalam autentikasi, *non-repudiation*, kerahasiaan, integritas atau ketersediaan dari sistem informasi.

2.2 *Framework* Manajemen Risiko

2.3.1 ISO/IEC 27005

Berdasarkan ISO/IEC 27005 [2] proses manajemen risiko terdiri dari 6 proses, yaitu:

Menetapkan konteks

Konteks dalam proses manajemen risiko harus ditetapkan yang meliputi kebutuhan dasar kriteria manajemen risiko, menentukan lingkup dan batasan serta membangun organisasi untuk proses *Information Security Risk Management* (ISRM).

Penilaian risiko

Penilaian risiko menentukan nilai dari aset informasi, mengidentifikasi ancaman yang dapat terjadi terhadap kelemahan yang ada, mengidentifikasi kontrol yang diterapkan, menentukan potensi konsekuensi dan menentukan prioritas terhadap risiko untuk dilakukan evaluasi sesuai dengan konteks yang telah ditetapkan.

***Treatment* risiko**

Treatment risiko berisi identifikasi dari sejumlah pilihan untuk melakukan *treatment* risiko, memberikan penilaian, persiapan dan implementasi rencana *treatment*.

Penerimaan risiko

Pada bagian ini difokuskan pada keputusan untuk menerima atau menolak terhadap *level* sisa risiko, berdasarkan pada *threshold* yang masih dapat diterima. Fase ini dipacu oleh fakta-fakta yang tidak masuk dalam *account*. *Output* dari setiap proses adalah daftar risiko yang diterima sesuai dengan kriteria penerimaan risiko suatu organisasi

Komunikasi risiko

Hal ini berupa dialog dengan para *stakeholder* untuk melakukan konsultasi guna mendapatkan informasi dua arah dari pembuat keputusan terhadap *stakeholder* lainnya. Pendekatan tim konsultatif digunakan untuk membantu mendefinisikan konteks secara tepat, membantu memastikan risiko telah diidentifikasi secara efektif, membedakan keahlian dalam menganalisis risiko, memastikan perbedaan pendapat dalam mengevaluasi risiko dan untuk merubah menajemen secara tepat pada saat *treatment* risiko.

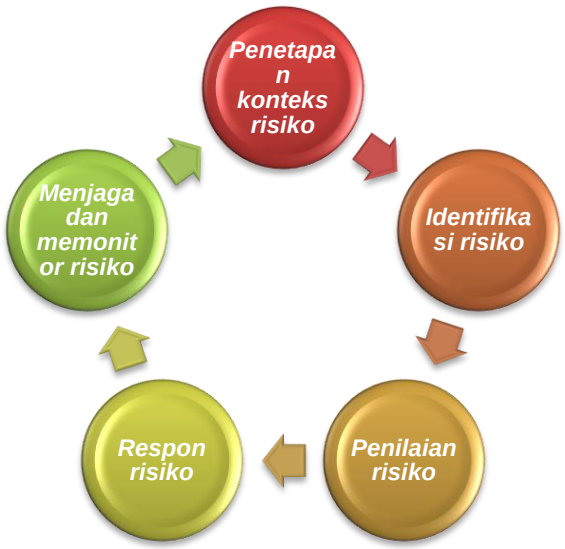
Pemantauan dan peninjauan risiko

Pada saat melakukan review hal yang penting adalah memastikan kesesuaian rencana manajemen risiko. Faktor-faktor yang mempengaruhi *likelihood* dan konsekuensi hasil dapat berubah, seperti faktor-faktor yang mempengaruhi biaya *treatment*. Pemantauan dan peninjauan juga merupakan pembelajaran dari proses manajemen risiko dengan

melakukan *review* kejadian, melakukan rencana *treatment* dan hasil.

2.3.2 COBIT

Referensi mengenai manajemen risiko secara khusus dibahas pada proses PO9 dalam COBIT. Proses-proses yang lain juga menjelaskan tentang manajemen risiko namun tidak terlalu detail. *Framework* manajemen risiko TI dengan menggunakan COBIT dapat dilihat pada gambar 2, yang terdiri dari [3] :



Gambar 2. Framework COBIT

Penetapan Konteks Risiko

Menetapkan konteks dimana kerangka kerja penilaian risiko diterapkan untuk memastikan hasil yang sesuai. Termasuk menentukan konteks internal dan eksternal setiap penilaian risiko, tujuan penilaian, dan kriteria risiko yang akan dievaluasi.

Identifikasi Risiko

Identifikasi risiko (ancaman nyata yang dapat mengeksploitasi kelemahan yang signifikan) dengan kecenderungan dampak negatif pada tujuan atau operasional perusahaan, termasuk bisnis, peraturan, hukum, teknologi, mitra niaga, sumberdaya manusia dan aspek operasional. Menentukan sifat dampak tersebut dan menjaga informasi ini. Mencatat dan menyimpan risiko yang relevan dalam daftar risiko. Identifikasi risiko merupakan proses untuk mengetahui risiko. Sumber risiko bisa berasal dari manusia, proses, dan teknologi, internal (dari dalam perusahaan) dan eksternal (dari luar perusahaan), bencana (*hazard*), ketidakpastian (*uncertainty*) dan kesempatan (*opportunity*).

Penilaian Risiko

Penilaian risiko adalah proses untuk menilai seberapa sering risiko terjadi atau seberapa besar dampak dari risiko. Dampak risiko terhadap bisnis (*business impact*) bisa berupa: dampak terhadap *financial*, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data), dan penundaan proses pengambilan keputusan. Penilaian dilakukan secara berulang. Sedangkan kecenderungan (*likelihood*) terjadinya risiko dapat disebabkan oleh sifat alami dari bisnis, struktur dan budaya organisasi, sifat alami dari sistem (tertutup atau terbuka, teknologi baru dan lama), dan kendali-kendali yang ada. Proses penilaian risiko bisa dilakukan dengan menggunakan metode kualitatif ataupun kuantitatif. Proses penilaian risiko bisa berupa risiko yang tidak dapat dipisahkan (*inherent risks*) dan sisa risiko (*residual risks*).

Respon Risiko

Respon risiko adalah proses untuk melakukan langkah-langkah yang diperlukan terhadap risiko. Respon terhadap risiko dilakukan dengan menerapkan kontrol objektif yang sesuai dalam melakukan manajemen risiko. COBIT juga menjelaskan bahwa untuk melakukan proses respon risiko dapat dilakuan dengan *avoidance, reduction, sharing* atau *acceptance.* Selain itu juga menentukan orang yang bertanggungjawab dan tingkat toleransi risiko. Jika sisa risiko masih melebihi risiko yang dapat diterima (*acceptable risks*), maka diperlukan respon risiko tambahan.

Menjaga dan Monitor Risiko

Memprioritaskan dan merencanakan aktivitas kontrol di semua tingkatan dalam mengimplementasikan respon risiko yang diidentifikasi dan diperlukan, termasuk identifikasi biaya-biaya, manfaat dan tanggung jawab pelaksanaan. Memperoleh persetujuan untuk melakukan tindakan yang disarankan dan penerimaan residu risiko, dan memastikan bahwa tindakan yang dilakukan menjadi tanggung jawab pemilik proses. Memantau pelaksanaan rencana, dan melaporkan setiap penyimpangan kepada manajemen senior

3. PEMODELAN MANAJEMEN RISIKO TI

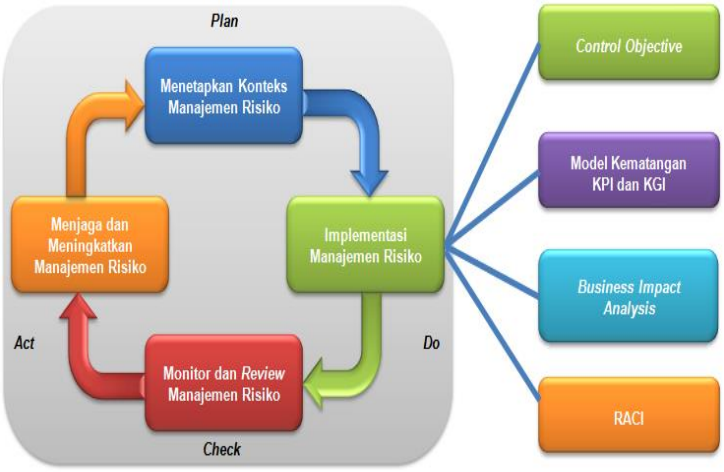
Secara umum model usulan proses manajemen risiko TI terdiri dari empat proses utama yang relevan dengan model *Plan, Do, Check, Act* (PDCA) yang ditunjukkan pada tabel 1.

Tabel 1. Relevansi proses manajemen risiko dan model PDCA

Proses Manajemen	Proses Manajemen Risiko
Plan	Menetapkan konteks manajemen risiko
Do	Implementasi manajemen risiko
Check	Monitor dan *review* manajemen risiko
Act	Menjaga dan meningkatkan manajemen risiko

Secara keseluruhan model manajemen risiko TI untuk keberlanjutan layanan TI dapat ditunjukkan pada gambar 3. Pada gambar 3, dapat dijelaskan

terdapat proses lain yang digunakan untuk mengukur kematangan proses, menentukan *control objective* dari proses, menentukan pelaksana proses dengan *Responsibility*, *Accountability*, *Consulted*, dan *Informed (*RACI), menentukan *Key Performance Indicator* (KPI) dan *Key Goal Indicatior* (KGI) serta menentukan BIA untuk keselarasan dengan rencana keberlanjutan bisnis perusahaan.



Gambar 3. Model usulan manajemen risiko TI

3.1 Implementasi Model Manajemen Risiko TI

Proses implementasi model manajemen risiko TI dilakukan dengan mengkategorikan kedalam lima proses utama yaitu mengkomunikasikan dan konsultasi risiko, menetapkan konteks, penilaian risiko, mitigasi risiko, pengawasan dan peninjauan risiko. Proses-proses tersebut dapat ditunjukan pada gambar 4. Penjelasan dari setiap proses yang dilakukan adalah sebagai berikut:

Menetapkan konteks

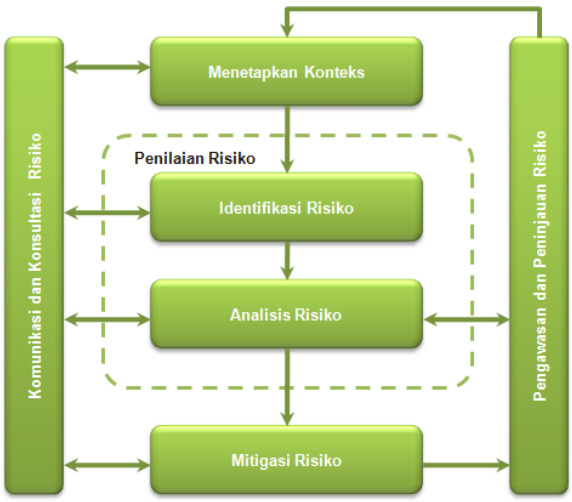
Menetapkan konteks merupakan kegiatan untuk memahami strategi, keorganisasian dan ruang lingkup manajemen risiko. Pada tahap ini tujuan dari *stakeholder* internal dan eksternal didefinisikan. Penentuan kriteria risiko yang ditetapkan akan dievaluasi dan menentukan analisis risiko secara terstruktur. Hal yang dilakukan dalam menentapkan konteksi risiko terdiri dari membangun konteks strategi dan organisasi dengan melakukan analisis *Strenght*, *Weakness*, *Opportunities*, *Threat* (SWOT), membangun konteks manajemen risiko, serta mengidentifikasi *stakeholder*.

Penilaian risiko

Penilaian risiko dilakukan untuk mengidentifikasi risiko-risiko yang timbul dan berdampak pada layanan TI, melakukan analisis terhadap identifikasi tersebut dan menentukan nilai terhadap risiko yang ditimbulkan sehingga dapat diketahui seberapa besar *exposure* dari risiko tersebut. Penilaian risiko tersebut dapat dilakukan dengan menggunakan metode kualitatif ataupun kuantitatif.

Mitigasi risiko

Pada tahap ini menerima dan mengawasi prioritas risiko rendah. Untuk risiko dengan nilai 8 keatas membutuhkan rencana tindakan manajemen lebih spesifik yang mempertimbangkan biaya (*cost*) yang harus dikeluarkan. Pilihan-pilihan mitigasi risiko dapat dilakukan dengan cara menghindari risiko, mereduksi kecenderungan risiko, mereduksi konsekuensi/dampak, dan mentransfer risiko.



Gambar 4. Proses manajemen risiko TI

Komunikasi dan konsultasi risiko

Melakukan komunikasi dan konsultasi dengan *stakeholder* internal dan eksternal untuk setiap proses manajemen risiko dan fokus pada proses keseluruhan. Rencana komunikasi harus dibangun untuk stakeholder internal dan eksternal di awal rencana proses manajemen risiko. Komunikasi seharusnya dua arah sehingga memudahkan untuk konsultasi. Manajemen bertanggungjawab untuk mengidentifikasi keberadaan risiko dan memastikan bahwa penanganan risiko telah dilakukan dengan tepat

Pengawasan dan peninjauan risiko

Pada tahap ini melakukan pengawasan dan meninjau efektivitas dan kinerja dari opsi mitigasi risiko, strategi, perubahan pada sistem manajemen yang dapat mempengaruhi hal tersebut.

3.2 Penilaian Risiko

Pada proses penilaian risiko dilakukan dengan dua tahap yaitu mengidentifikasi risiko dan menganalisis risiko.

3.2.1 Identifikasi Risiko

Mengidentifikasi apa, mengapa, dan bagaimana risiko dapat meningkat sebagai dasar untuk analisis. Tahapan ini harus mengidentifikasi seluruh risiko yang muncul dari hasil identifikasi lingkungan operasional dan menetapkan daftar risiko yang dapat memberikan dampak pada layanan TI. Pada tahapan ini terbagi menjadi tiga bagian. Tahapan pertama mengidentifikasi aset yang dimiliki oleh perusahaan

yang disusun kedalam katalog aset, tahapan kedua mengidentifikasi ancaman yang mungkin terjadi dalam layanan TI yang disusun kedalam katalog sumber ancaman, dan tahapan ketiga yaitu mengidentifikasi kelemahan yang dimiliki dan disusun dalam katalog kelemahan. Ketiga katalog tersebut dapat dilihat pada tabel 2-4.

Tabel 2. Katalog aset

Katalog Aset	
Aplikasi	Aplikasi untuk proses bisnis
Informasi	Data dan Informasi
Infrastruktur	Sistem Operasi
	Database Management System
	Hardware
	Jaringan Komunikasi
	Auxiliary equipments
	Fasilitas Fisik
Sumberdaya manusia	Personil

Tabel 3. Katalog sumber ancaman

No	**Katalog Sumber Ancaman (*threat source*)**
Kejadian Alam	
1	Kebakaran
2	Banjir
3	Halilintar
	…
Faktor Lingkungan atau Kesalahan Teknis	
1	Kerusakan saluran air
2	Interferensi elektromagnetik dari peralatan
3	Ledakan elektromagnetik industri
	…
Human Accidental	
1	Kesalahan pengguna
2	Kesalahan administrator
3	Kesalahan konfigurasi
	…
Human Deliberate (malicious)	
1	Spionase/ mata-mata (menggunakan sumberdaya penting)
2	*Vandalism* dari luar dan dari dalam
3	Terorisme: sabotase, peledakan bom
4	Pencurian *hardware* dan peralatan jaringan
5	*Malicious* yang menghapus konfigurasi jaringan dan *hardware*
6	Kerusakan jaringan yang diakibatkan oleh *worm*
7	*Malicious* dan penurunan sumberdaya TI oleh kelompok pengguna
8	Distorsi pemasukan data atau *fiddling of data*
9	Penghapusan secara intensif (langung atau tidak langsung), pencurian atau penghancuran program atau konten data
10	Akses tidak terototisasi terhadap data atau informasi
11	Pencurian dokumen atau media
12	*Malicious* yang menghapus file dalam penyimpanan
13	Modifikasi *malicious* (langsung atau tidak langsung) terhadap fungsionalitas program atau operasional program
14	Penggunaan *software* ilegal
15	Penyusupan ke sistem oleh pihak ketiga yang bekerja sama dengan organisasi
16	*Malicious* yang menghapus konfigurasi *software*
	…

Tabel 4. Katalog Kelemahan

No	**Deskripsi Kelemahan (*vulnerability*)**
Hardware	
1	Kegagalan instalasi media penyimpanan
2	Sensitif terhadap radiasi elektromagnetik
3	Jadwal penggantian yang tidak tepat waktu
4	Kekurangan kontrol perubahan konfigurasi
5	Kelemahan terhadap tidak stabilnya *powersupply*
	…
Software	
1	Pengujian *software* yang tidak cukup
2	Lemah terhadap jejak audit
3	Penggunaan kembali media penyimpanan tanpa penghapusan yang tepat
4	Kesalahan alokasi pengaksesan
5	Terdapat *bug*
6	Tampilan *interface* yang kompleks
	…
Jaringan	
1	Lemahnya identifikasi dan mekanisme autentifikasi
2	*Password* tidak terlindungi
3	Manajemen *password* yang buruk
4	Penerapan *service* yang tidak diperlukan
5	Penggunaan *software* baru
6	Lemahnya kontrol perubahan
7	Tidak terkontrolnya *download* dan penggunaan *software*
8	Lemahnya *backup* data
9	Kegagalan manajamen pelaporan
10	Saluran komunikasi yang tidak aman
11	Lemahnya identifikasi dan autentifikasi pengirim dan penerima
	…
Personal	
1	Staf tidak hadir
2	Prosedur rekruitmen yang buruk
3	Pelatihan keamanan tidak mencukupi
4	Kesalahan penggunaan *software* dan *hardware*
5	Kurangnya kesadaran keamanan
6	Kurangnya mekanisme pengawasan
	…
Internal Organisasi	
1	Kurangnya kontrol terhadap akses fisik misalnya gedung, ruangan
2	Lokasi area yang rawan banjir
3	Sumber tenaga yang tidak stabil
4	Kurangnya perlindungan terhadap gedung
5	Kurangnya prosedur formal untuk registrasi dan de-registrasi
6	Lemahnya kontrak dengan *customer* atau pihak ketiga
7	Kurangnya prosedur pengawasan pemrosesan informasi
8	Kurangnya audit berkala
9	Kurangnya prosedur untuk identifikasi dan penilaian risiko
10	Kurangnya prosedur kontrol perubahan
11	Kurangnya rencana keberlanjutan
	…

keterangan

… = terdapat detail katalog lebih lanjut

3.2.2 Analisis Risiko

Tujuan dari tahap ini adalah untuk menganalisis risiko dari hasil identifikasi sebelumnya. Pada tahap ini dianalisis mengenai kontrol yang sudah diterapkan perusahan, menentukan kecenderungan

(*likelihood*), dan menentukan dampak (*impact*). Setelah kecenderungan dan dampak telah diketahui, dapat dilakukan estimasi tingkat risiko yang terjadi dengan menggunakan persamaan 1.

Risiko = kecenderungan x dampak (1)

Pada penelitian ini, estimasi penilaian risiko dilakukan dengan memberikan rentang nilai skala yang terdiri dari *extreme, high, medium,* dan *low risk* yang dapat dijelaskan serta dipetakan dalam tabel 5 sebagai berikut:

1. *Nilai >9* : Sangat tinggi (*Very high/Extreme risk*)
   Membutuhkan rencana tindakan yang lebih rinci
2. *Nilai >6* : Tinggi (*High risk*)
   Membutuhkan perhatian manajemen senior
3. *Nilai 5,6* : Sedang (*Medium risk*)
   Penanggungjawab manajemen risiko secara spesifik
4. *Nilai <5:* Rendah (*Low risk*) Dikelola dengan prosedur rutin

Tabel 5. Penilaian risiko

Dampak (*Impact*)		Kecenderungan (*Likelihood*)				
		Tidak mungkin	Jarang	Kadang	Mungkin	Sering
		1	2	3	4	5
Sangat tinggi	4	4	8	12	16	20
Tinggi	3	3	6	9	12	15
Sedang	2	2	4	6	8	10
Rendah	1	1	2	3	4	5

3.3 Pengujian Model Manajemen Risiko

Setelah model manajemen risiko TI berhasil dirancang, selanjutnya dilakukan pengujian terhadap setiap komponen model. Uji model yang dilakukan yaitu dengan menggunakan metode statistik. Untuk menguji apakah setiap instrumen layak atau tidak dilakukan uji validitas dan uji reliabilitas. Setelah uji validitas dan reliabilitas berhasil dilakukan selanjutnya dilakukan pengujian model dengan melakukan survey lapangan dengan cara memberikan kuesioner kepada 48 responden. Dari data yang berhasil dikumpulkan selanjutnya dilakukan analisis data dengan menggunakan metode korelasi Pearson, analisis regresi dan analisis regresi ganda untuk menguji hubungan dari setiap komponen model seperti yang dicontohkan pada tabel 6. Dari tabel 6 tersebut dapat dijelaskan dengan tingkat signifikansi 0,001 dan nilai korelasi 0,477 menunjukan bahwa terdapat hubungan antara penilaian risiko dengan BIA.

Dari hasil uji statistik yang telah dilakukan terhadap seluruh komponen model dapat dibuat kesimpulan bahwa model manajemen risiko TI untuk keberlanjutan layanan TI telah divalidasi dan diuji sehingga model dapat diimplementasikan.

Tabel 6. Hasil Pengujian korelasi metode Pearson antara penilaian risiko dengan BIA

Metode	Komponen Uji		Nilai Korelasi	Nilai Signifikansi (p)	Keputusan
Pearson Correlation	Penilaian Risiko	BIA	0,477	0,001	Ho ditolak

4. KESIMPULAN

Kesimpulan yang diperoleh dari penelitian yang telah dilakukan sebagai berikut:

Pembangunan model manajemen risiko TI untuk keberlanjutan layanan TI telah berhasil dilakukan dengan menetapkan sejumlah proses yang dapat dilakukan untuk manajemen risiko TI. Model manajemen risiko TI untuk keberlanjutan layanan TI telah berhasil diuji dan divalidasi dengan menggunakan uji statistik. Metode Pearson, analisis regresi, dan analisis regresi ganda digunakan sebagai metode untuk pengujian. Dari hasil pengujian tersebut dapat ditetapkan bahwa model dapat diterapkan atau diimplementasikan.

5. DAFTAR PUSTAKA

[1] Hiles, A.,2002, *Enterprise Risk Assessment and Business Impact Analysis*, Rothstein Assoc

[2] ISO/IEC, 2008, *ISO/IEC 27005 : Information Technology - Security Techniques – Information Security Risk Management*, British Standard.

[3] ITGI, 2007, *COBIT 4.1 : Framework, Control Objective, Management guideline, Maturity Model*, IT Governance Institute.

[4] Kouns, J. d, 2010, *Information Technology Risk Management in Enterprise Environments*, John Wiley and Sons.

[5] Maulana, M. dan Supangkat, S., 2006, Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, (pp. 121-126), Bandung.

[6] Publicas, M, 2006, Magerit Version 2 - Methodology for Information System Risk Analysis and Management: I - The Method. Ministerio de Administraciones Publicas.

[7] Priyadi, Y., 2008, *Perancangan Instrumen Pengukuran Risk Assessment Sebagai Rekomedasi Strategi Mitigas Risiko di SPBU Bandung*, ITB

[8] Stoneburner, G., 2002, *Risk Management Guide for Information Technology System*, National Institute of Standards and Technology Special Publication 800-30.

[9] Spremic, M., and Popovic, M., 2008, Emerging issues in IT Governance: Implementing the Corporate IT Risk Management Model, *WSEAS Transacions on Systems, issues 3 Volume 7*