MODEL PENGELOLAAN RISIKO TI MENGGUNAKAN *RISK IT* DI ITENAS BANDUNG

R. Budiraharjo

Jurusan Teknik Informatika, Fakultas Teknologi Industri, Institut Teknologi Nasional Bandung
Institut Teknologi Nasional, Jl. PKH Mustafa No. 23 Bandung 40124
[1] budiraharjo@itenas.ac.id

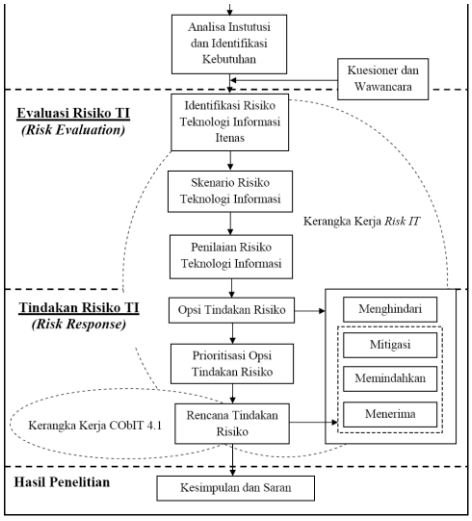
Abstrak

Kehandalan mengelola teknologi informasi menentukan keberhasilan institusi dalam menghasilkan suatu informasi yang utuh, aman, konsisten, tepat waktu , dan relevan. Dengan demikian informasi yang dihasilkan dapat mendukung proses pengambilan keputusan dan operasional kegiatan di Itenas. Namun, penggunaan teknologi informasi selain meningkatkan kecepatan dan keakuratan serta pelayanan, juga meningkatkan risiko misalnya risiko operasional, reputasi, kepatuhan dan strategis. Untuk itu Itenas dituntut untuk memiliki manajemen risiko yang terpadu dalam melakukan identifikasi, pengukuran, dan pengendalian risiko teknologi informasi. *Risk IT Framework*, adalah kerangka kerja yang dinilai sesuai dengan model yang ingin diterapkan di Itenas karena memandang pengelolaan risiko teknologi informasi sebagai pengelolaan yang terintegrasi dalam pengelolaan strategis organisasi secara keseluruhan. Namun, *Risk IT Framework* tidak mencakup kegiatan-kegiatan mitigasi risiko TI, oleh karena itu rencana mitigasi risiko-risiko teknologi informasi yang teridentifikasi dalam penelitian ini dibuat dengan mempergunakan control objectives dari kerangka kerja CObIT 4.1.

Kata kunci: Pengelolaan risiko teknologi informasi, *Risk IT framework*, CObIT 4.1, mitigasi risiko.

1. Pendahuluan

Perguruan tinggi merupakan sebuah institusi dengan salah satu tugas yang diembannya adalah memberikan pelayanan kepada masyarakat untuk menyiapkan Sumber Daya Manusia (SDM) masa depan yang bermutu dan berdaya guna. Salah satu cara untuk menciptakan daya saing untuk sebuah Perguruan Tinggi adalah dengan pemanfaatan teknologi informasi (TI), untuk menunjang aktivitasnya. Oleh karena itu, pengembangan implementasi teknologi informasi di perguruan tinggi merupakan upaya yang sudah seharusnya dilakukan. Risiko yang timbul akibat penerapan TI yang salah akan menyebabkan proses bisnis yang tidak optimal, kerugian finansial, menurunnya reputasi organisasi, atau bahkan hancurnya bisnis organisasi. Oleh karena itu diperlukan suatu pengukuran terhadap risiko penerapan TI bagi organisasi. Pengukuran risiko TI berguna untuk mengetahui profil resiko TI, analisa terhadap risiko, kemudian melakukan respon terhadap risiko tersebut sehingga tidak terjadi dampak-dampak yang dapat ditimbulkan oleh risiko tersebut. Terdapat banyak metode atau kerangka kerja (*framework*) yang bisa dijadikan sebagai *best practice* dalam penerapan manajemen risiko TI, salah satunya adalah *Risk IT Framework*. *Risk IT* mempunyai tujuan untuk membantu organisasi dalam mengidentifikasi dan mengelola risiko terhadap aset teknologi informasinya. *Risk IT* merupakan sebuah kerangka kerja manajemen risiko teknologi informasi yang dibuat selaras serta saling melengkapi dengan kerangka kerja CobIT dan kerangka kerja Val IT. Keselarasan yang dimaksud adalah dalam hal CobIT menawarkan beberapa kegiatan pengendalian untuk mitigasi resiko teknologi informasi pada prosesnya, sedangkan Val IT ditujukan untuk membantu organisasi-organisasi dalam membuat keputusan mengenai dimana investasi teknologi informasi seharusnya dilakukan. Metodologi dalam penelitian ini adalah sebagai berikut.



Gambar 1: Kerangka Penelitian

2. Pengelolaan Risiko TI

2.1 Risiko Teknologi Informasi

Sasaran dari pelaksanaan manajemen risiko TI adalah untuk mengurangi risiko yang berbeda-beda yang berkaitan dengan bidang yang telah dipilih pada tingkat yang dapat diterima. Hal ini dapat berupa berbagai jenis ancaman yang disebabkan oleh lingkungan, teknologi, manusia, organisasi dan politik. Di sisi lain, pelaksanaan pengelolaan risiko melibatkan segala cara yang tersedia bagi manusia, khususnya, bagi entitas pengelolaan risiko (manusia, staff, dan organisasi).

Pengelolaan risiko TI dimulai dari proses identifikasi resiko, penilaian risiko, mitigasi, monitoring dan evaluasi. Teknologi informasi merupakan aset penting dalam operasional yang dapat meningkatkan nilai tambah dan daya saing organisasi sementara dalam penyelenggaraannya mengandung berbagai risiko, maka organisasi perlu menerapkan pengelolaan risiko TI. Keberhasilan penerapan pengelolaan risiko TI tersebut sangat tergantung pada komitmen seluruh unit kerja di organisasi tersebut, baik penyelenggara maupun pengguna teknologi informasi. Penerapan pengelolaan risiko TI yang efektif dilakukan melalui penyelarasan Rencana Strategis Teknologi Informasi dengan strategi bisnis organisasi, optimalisasi pengelolaan sumber daya, pemanfaatan teknologi informasi (*IT value delivery*), serta pengukuran kinerja.

Risiko TI dapat dikategorikan dalam berbagai cara, yaitu:

1. Risiko pemanfaatan teknologi informasi, yang terkait dengan penggunaan teknologi untuk meningkatkan efisiensi dan efektifitas proses bisnis, atau sebagai wahana untuk menciptakan peluang bisnis baru.
2. Risiko penyelesaian program dan proyek teknologi informasi, yang terkait dengan kontribusi TI terhadap solusi bisnis yang ditingkatkan atau baru yang biasanya dalam bentuk program kegiatan dan proyek.
3. Risiko operasional dan layanan TI, yang terkait dengan semua hal mengenai kinerja sistem dan layanan TI yang dapat merugikan organisasi.

2.2 Risk IT dan CObIT dalam Pengelolaan Risiko TI

Kerangka kerja *Risk IT* merupakan kerangka khusus pengelolaan risiko bisnis terkait dengan penggunaan teknologi informasi (TI) yang merupakan penyempitan dari kerangka kerja CObIT.

Sasaran dari pengelolaan risiko TI menurut *Risk IT* adalah:

1. Mengintegrasikan pengelolaan risiko TI kedalam ERM secara keseluruhan sehingga organisasi dapat membuat keputusan-keputusan yang sadar akan resiko dan manfaatnya.
2. Membuat keputusan yang berdasarkan informasi yang baik mengenai akibat dari risiko, serta sesuai dalam cakupan *risk appetite* dan *risk tolerance* dari organisasi
3. Mampu untuk menindak lanjuti risiko terkait teknologi informasi.

Pengelolaan risiko TI menurut *Risk IT* mengikuti prinsip-prinsip berikut ini:

1. Selalu berkaitan dengan tujuan bisnis
2. Menyelaraskan pengelolaan risiko TI bisnis dengan ERM (Manajemen Resiko Organisasi) secara keseluruhan
3. Menyeimbangkan anatar biaya dan keuntungan akan pengelolaan risiko TI
4. Mengedepankan keseimbangan dan keterbukaan komunikasi mengenai risiko TI
5. Menciptakan komitmen manajemen atas serta menjabarkan dan menerapkan akuntabilitas di level bawah untuk bekerja dalam cakupan toleransi yang dapat diterima.
6. Sebuah proses yang berkesinambungan dan merupakan bagian dari kegiatan sehari-hari

CobIT merupakan kerangka kerja pengendalian internal yang berkaitan dengan teknologi informasi, yang dipublikasikan oleh Information System Audit and Control Foundation di tahun 1996 dan di-update pada tahun 1998 dan 2000. CobIT dibuat dengan tujuan melakukan penelitian dan pengembangan terhadap sekumpulan kontrol teknologi informasi, yang dapat diterima secara internasional bagi kepentingan auditor dan manajer bisnis suatu organisasi.

Proses dalam kerangka kerja CobIT 4.1 yang mengelola risiko Teknologi Informasi adalah *PO9 Asses and Manage IT Risks*. Menurut CobIT 4.1, pengelolaan risiko teknologi informasi memerlukan sebuah kerangka kerja agar dapat berhasil dengan baik. Ancaman-ancaman potensial terhadap tujuan organisasi yang disebabkan oleh suatu peristiwa yang tidak direncanakan harus diidentifikasi, dianalisa, dan dinilai. Setelah itu, perlu dirancang strategi mitigasi risiko yang sesuai untuk meminimalkan risiko ke tingkat yang dapat diterima. Hasil pengukuran risiko hendaknya disampaikan kepada para pemangku kepentingan dengan menggunakan bahasa yang dapat dimengerti dan dinyatakan keterkaitannya dengan masalah keuangan, sehingga para pemangku kepentingan dapat menyelaraskan risiko ke tingkat yang dapat diterima.

3. Analisa Risiko TI Itenas

3.1. Identifikasi Risiko TI

Berdasarkan hasil kuesioner, terdapat 14 (empat belas) risiko-risiko generik teknologi informasi yang terbagi atas lima kategori risiko, yaitu Risiko Proses Bisnis, Risiko Teknologi, Risiko, Risiko Manusia, Risiko Kerusakan

Infrastruktur, dan Risiko Alam di Institut Teknologi Nasional Bandung. Risiko-risiko tersebut adalah:

a. 3 Risiko Proses Bisnis: (1) Kesalahan pemilihan penyedia sistem, (2) Ketidak patuhan penyedia sistem terhadap kesepakatan kontrak, (3) Integrasi teknologi informasi dengan proses bisnis;
b. 5 Risiko Teknologi: (4) Kerusakan perangkat lunak dan data, (5) Serangan sistem, (6) Kerusakan alat, (7) Ketiadaan daya, (8) Infeksi virus komputer;
c. 3 Risiko Manusia: (9) Pencurian, (10) Kesalahan operasional, (11) Keterampilan staf TI;
d. 2 Risiko Kerusakan Infrastruktur: (12) Kebakaran, (13) Kerusakan gedung, dan;
e. 1 Risiko Alam: (14) Infrastruktur TI rusak atau tidak berfungsi akibat bencana alam.

3.2. Skenario Risiko TI

Pada tahapan ini, risiko-risiko yang telah teridentifikasi dipetakan kedalam sebuah skenario risiko dengan mengadaptasi pemetaan skenario risiko dari kerangka kerja *Risk IT*. Menurut pola pikir kerangka kerja Risk IT, penyusunan skenario risiko teknologi informasi hendaknya mempertimbangkan beberapa komponen risiko. Komponen-komponen tersebut adalah:

1. Aktor/pelaku (*actor*)
2. Jenis ancaman (*threat type*)
3. Kejadian (*event*)
4. Aset dan sumber daya (*asset/resources*)
5. Waktu (*time*)

Gambar dibawah ini menggambarkan hubungan komponen-komponen risiko terhadap skenario risiko.

Gambar 2: Komponen skenario risiko [13]

3.3. Penilaian Risiko TI

Pada tahap ini, risiko-risiko yang telah dianalisis pada bagian sebelumnya akan dinilai berdasarkan frekuensi terjadinya risiko dan dampak risiko terhadap keberlangsungan bisnis. Penilaian yang dilakukan mengadaptasi cara berpikir kerangka kerja *Risk IT*. Nilai frekuensi risiko (F) dan dampak risiko (D) akan dinyatakan dinyatakan dengan angka 1 hingga 5. Penjelasannya dapat dilihat pada Tabel 1 dan Tabel 2 sebagai berikut.

Nilai (F)	Frekuensi	Keterangan
5	Sangat Tinggi	Terjadi 11 hingga 100 kali setiap 1 tahun
4	Tinggi	Terjadi 3 hingga 10 kali setiap 1 tahun
3	Sedang	Terjadi 1 hingga 4 kali setiap 4 tahun
2	Rendah	Terjadi 1 hingga 2 kali setiap 10 tahun
1	Sangat Rendah	Terjadi 1 hingga 9 kali setiap 100 tahun

Tabel 1: Skala Frekuensi Risiko TI

Nilai (D)	Dampak	Keterangan
5	Sangat Tinggi	Sangat menggangu kelangsungan proses bisnis organisasi dan atau mengakibatkan kerugian finansial yang sangat besar
4	Tinggi	Menggangu kelangsungan proses bisnis organisasi dan atau mengakibatkan kerugian finansial yang besar
3	Sedang	Cukup menggangu kelangsungan proses bisnis organisasi dan atau mengakibatkan kerugian finansial yang tidak terlalu besar
2	Rendah	Berpotensi menggangu kelangsungan proses bisnis organisasi dan atau berpotensi mengakibatkan kerugian finansial yang tidak terlalu besar
1	Sangat rendah	Hampir tidak menggangu kelangsungan proses bisnis organisasi dan atau hampir tidak mengakibatkan kerugian finansial.

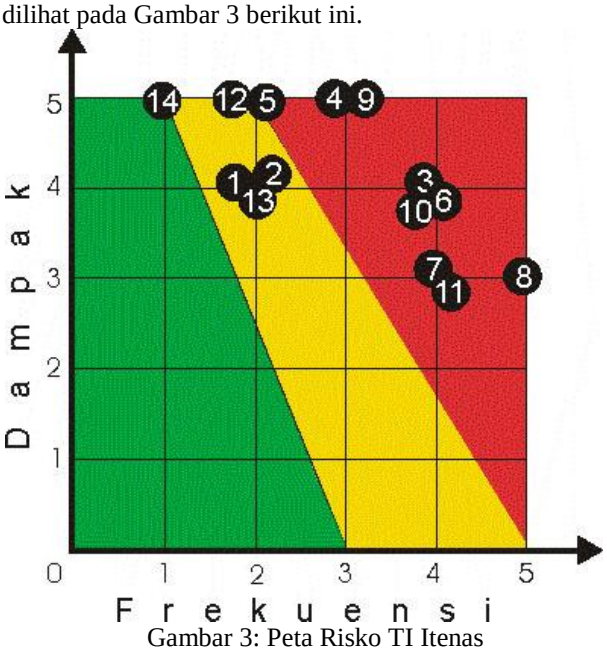
Tabel 2: Skala Dampak Risiko TI

Risiko-risiko teknologi informasi yang telah diberi nilai frekuensi (F) dan dampaknya (D) kemudian diberikan skor dengan menggunakan Tabel Skala Penilaian seperti pada Tabel 3 sebagai berikut.

Rumus (D x F)		Dampak (D)				
		1	2	3	4	5
Frekuensi (F)	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Tabel 3: Skala Penilaian Risiko TI

Dari hasil penilaian, kemudian risiko dipetakan kedalam sebuah peta risiko. Peta risiko yang dipergunakan mengadaptasi *risk mapping tool* kerangka kerja Risk IT. Hasil pemetaannya dapat dilihat pada Gambar 3 berikut ini.



Gambar 3: Peta Risko TI Itenas

Hasil penilaian dan pemetaan risiko-risiko teknologi informasi kemudian di berikan peringkat berdasarkan nilai risiko. Tabel 4 menjelaskan peringkat risiko TI di Itenas.

Rank	Risiko	Ketegori Risiko
1	Integrasi IT dengan proses bisnis (3)	Risiko Tinggi
2	Kerusakan alat (6)	Risiko Tinggi
3	Kesalahan operasional (10)	Risiko Tinggi
4	Kerusakan perangkat lunak dan data (4)	Risiko Tinggi
5	Infeksi virus komputer (8)	Risiko Tinggi
6	Pencurian (9)	Risiko Tinggi
7	Ketiadaan daya *(Power outage)* (7)	Risiko Tinggi
8	Keterampilan staf TI (11)	Risiko Tinggi
9	Serangan sistem (5)	Risiko Tinggi
10	Kebakaran (12)	Risiko Tinggi
11	Kesalahan pemilihan penyedia sistem (1)	Risiko Sedang
12	Ketidak patuhan penyedia sistem terhadap kesepakatan kontrak (2)	Risiko Sedang
13	Kerusakan gedung (13)	Risiko Sedang
14	Bencana alam (14)	Risiko Rendah

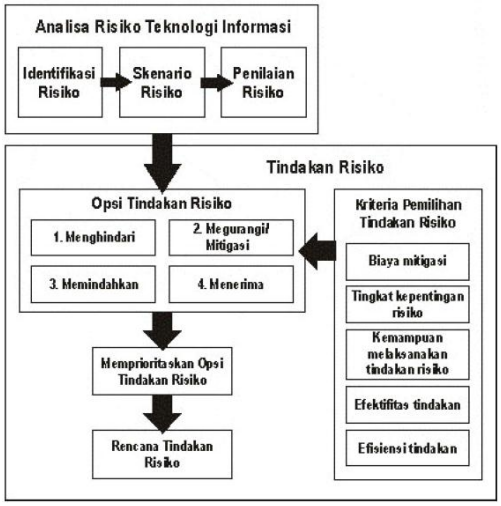
Tabel 4: Peringkat Risiko TI Itenas

4. Model Pengelolaan Risiko TI Itenas

4.1. Usulan Model Pengelolaan

Beberapa hal yang ingin dihasilkan dari model pengelolaan risiko adalah:

1. Model pengelolaan risiko untuk Teknologi Informasi Itenas dirancang mengadopsi kerangka kerja *Risk IT*.
2. Model pengelolaan risiko untuk Teknologi Informasi Itenas dirancang untuk menangani ancaman-ancaman yang telah dijabarkan pada analisis resiko dengan menggunakan pendekatan kualitatif.
3. Model pengelolaan risiko untuk Teknologi Informasi Itenas harus memenuhi kriteria-kriteria pemilihan tindakan risiko dengan memaksimalkan sumber daya Teknologi Informasi yang telah ada.
4. Model pengelolaan risiko untuk Teknologi Informasi Itenas terdokumentasi dengan baik dan mudah dipahami.
5. Model pengelolaan risiko untuk Teknologi Informasi Itenas mudah direvisi dan disesuaikan dengan perubahan yang mungkin akan terjadi.



Gambar 4: Usulan Model Pengelolaan Risiko TI Itenas

4.1. Prioritisasi Opsi Tindakan

Tujuan dari memprioritaskan opsi tindakan risiko teknologi informasi adalah untuk menyelaraskan risiko-risiko teknologi informasi terhadap batas toleransi risiko institusi. Penentuan jenis tindakan risiko terkait dengan kriteria-kriteria penentuan tindakan risiko dimana anggaran yang disediakan institusi untuk mengantisipasi kejadian risiko-risiko teknologi informasi merupakan faktor yang paling menetukan toleransi risiko.

Kegiatan ini bukan suatu kegiatan yang dapat diselesaikan hanya dalam satu kali pelaksanaan. Namun, kegiatan ini merupakan bagian dari siklus proses pengelolaan risiko teknologi informasi institusi. Dalam model pengelolaan risiko teknologi informasi menurut *Risk IT*, kegiatan ini dijabarkan dalam kegiatan RR2.3. (Melakukan Tindakan Terhadap Risiko yang Teridentifikasi).

Dalam model pengelolaan risiko teknologi informasi pada penelitian ini, terdapat empat opsi yang dapat dipilih untuk menindak lanjuti risiko-risiko teknologi informasi yang telah teridentifikasi dan dianalisa. Opsi-opsi tersebut adalah:

1. Menghindari risiko,
2. Mengurangi / mitigasi risiko,
3. Memindahkan risiko,
4. Menerima risiko.

Untuk menentukan opsi yang akan diterapkan untuk menindak lanjuti sebuah risiko, perlu dilakukan pengukuran dengan mempertimbangkan kriteria-kriteria pemilihan tindakan risiko. Kriteria-kriteria tersebut adalah:

1. Biaya
2. Tingkat kepentingan
3. Kemampuan melaksanakan
4. Efektifitas
5. Efisiensi.

4.1. Tindakan Risiko

Tindakan risiko akan dipilih berdasarkan nilai yang tertinggi, seperti yang dijelaskan pada Tabel 5.

	Risiko	Opsi Tindakan			
		Menghindari	Mitigasi	Memindahkan	Menerima
1.	Kesalahan pemilihan penyedia system				
2.	Ketidak patuhan penyedia sistem terhadap kesepakatan kontrak				
3.	Integrasi teknologi informasi dengan proses bisnis				
4.	Kerusakan perangkat lunak dan data				
5.	Serangan system				
6.	Kerusakan alat				
7.	Ketiadaan daya (*Power outage*)				
8.	Infeksi virus computer				
9.	Pencurian				
10.	Kesalahan operasional				
11.	Keterampilan staf TI				
12.	Kebakaran				
13.	Kerusakan gedung				
14.	Infrastruktur TI (software, hardware, data) rusak atau tidak berfungsi akibat bencana alam				

Tabel 5: Pemilihan Tindakan Risiko TI Itenas

Perancangan tindakan risiko mitigasi dalam penelitian ini menggunakan control objectives kerangka kerja CObIT 4.1.

5. Hasil Penelitian

5.1. Kesimpulan

Berdasarkan hasil penelitian ini dapat disimpulkan beberapa hal sebagai berikut.

1. Perancangan pengelolaan teknologi informasi Institut Teknologi Nasional Bandung dengan menggunakan kerangka kerja pengelolaan risiko teknologi informasi *Risk IT dalam* penelitian ini telah menghasilkan model pengelolaan yang sesuai dengan kebutuhan dan kondisi penerapan teknologi informasi di Institut Teknologi Nasional Bandung.
2. Penelitian ini telah berhasil menganalisa risiko teknologi informasi di Institut Teknologi Nasional Bandung, terdapat 14 (empat belas) risiko-risiko generik teknologi informasi yang terbagi atas lima kategori risiko, yaitu Risiko Proses Bisnis, Risiko Teknologi, Risiko, Risiko Manusia, Risiko Kerusakan Infrastruktur, dan Risiko Alam. Risiko-risiko tersebut adalah: (1) Kesalahan pemilihan penyedia sistem, (2) Ketidak patuhan penyedia sistem terhadap kesepakatan kontrak, (3) Integrasi teknologi informasi dengan proses bisnis, (4) Kerusakan perangkat lunak dan data, (5) Serangan sistem, (6) Kerusakan alat, (7) Ketiadaan daya, (8) Infeksi virus komputer, (9) Pencurian, (10) Kesalahan operasional, (11) Keterampilan staf TI, (12) Kebakaran, (13) Kerusakan gedung, dan (14) Infrastruktur TI rusak atau tidak berfungsi akibat bencana alam.
3. Setelah melalui proses penentuan opsi tindakan risiko dalam penelitian ini, tindak lanjut yang dipilih berdasarkan hasil penilaian empat belas risiko yang teridentifikasi adalah mitigasi (risiko) untuk risiko 1 hingga 11, memindahkan (risiko) untuk risiko 12 dan 13, serta menerima (risiko) untuk risiko 14.
4. Rekomendasi tindak lanjut mitigasi risiko yang dihasilkan dari penelitian ini dibuat dengan dengan menggunakan *control objectives* dari kerangka kerja CObIT 4.1. Sedangkan rekomendasi tindak lanjut memindahkan risiko adalah dengan menggunakan jasa pihak ketiga, dimana dalam konteks ini adalah perusahaan asuransi. Untuk risiko infrastruktur TI rusak atau tidak berfungsi akibat bencana alam, rekomendasi yang dibuat adalah menerima risiko dengan mempertimbangkan bahwa risiko

ini termasuk dalam kategori risiko rendah dalam matriks risiko dimana meskipun akan berdampak besar jika terjadi, namun frekuensi kejadian bencana alam yang berdampak langsung di Institut Teknologi Nasional Bandung sangat rendah.

5.2. Saran

Untuk perbaikan dan peningkatan penelitian di masa akan datang, maka beberapa saran diberikan, sebagai berikut:

1. Data untuk penelitian ini sebagian dihasilkan dari instrumen yang mendasarkan persepsi pada jawaban responden dimana responden yang dilibatkan adalah para pengelola teknologi informasi, dosen, dan mahasiswa. Pihak pimpinan, dalam hal ini adalah Rektor dan para Pembantunya masih belum dilibatkan sebagai responden. Hal ini dapat menimbulkan masalah jika persepsi responden yang dilibatkan dalam penelitian ini berbeda dengan persepsi dari sudut pandang pihak pimpinan. Oleh karena itu rancangan model pengelolaan risiko teknologi informasi Institut Teknologi Nasional Bandung perlu disempurnakan melalui *feedback* atau masukan yang diperoleh pada saat melakukan implementasi dengan melibatkan para pimpinan sebagai responden untuk penilitian selanjutnya.
2. Dalam penelitian ini, data dan teknologi pengelolanya (perangkat lunak) masih di gabungkan kedalam sebuah pengelolaan risiko. Pada penelitian selanjutnya, perlu dipisahkan antara pengelolaan risiko untuk data dengan teknologi pengelolanya, karena data merupakan aset teknologi informasi penting yang harus dilindungi.
3. Perlu adanya kesadaran dan komitmen dari pihak pimpinan Institut Teknologi Nasional Bandung dan jajarannya mengenai pentingnya menerapkan pengelolaan risiko teknologi informasi yang baik dan menyeluruh untuk mendukung kegiatan Institusi agar dapat memberikan pelayan terbaik bagi semua pemangku kepentingan. Penerapan pengelolaan risiko teknologi informasi ini disarankan dilaksanakan secara bertahap melalui manajemen perubahan yang baik sehingga Institusi dapat mengevaluasi efektifitas pengelolaan serta dapat melakukan perbaikan secara berkelanjutan.

Daftar Pustaka:

[1] Brandon, Dan (2006). *Project Management for Modern Information Systems*. U.S.A: IRM Press.

[2] Cabinet Office. (2008). *ITIL - Service Design Version.3*. United Kingdom: The Stationary Office.

[3] Chapman, Robert J. (2011). *Simple Tools and Techniques of Enterprise Risk Management 2nd Edition*. United Kingdom: John Wiley & Son, Ltd.

[5] Committee of Sponsoring Organisations of the Treadway Commission (COSO). (2004). *Enterprise Risk Mangement—Integrated Framework*.

[6] Fulmer, Kenneth L. (2005). *Business Continuity Planning: A Step-by-Step Guide with Planning Forms, Third Edition.* Rothstein Associates.

[8] Grembergen,Win Van. (2004). *Strategies for Information Technology Governance*, Idea Group Publishing.

[9] Harrington, Scott E., & Nichaus, Gregory R.(2004) *Risk Management and Insurance (2nd Edition)*. Singapore : McGraw-Hill.

[10] International Organisation for Standardisation. (2005). *ISO/IEC 17799:2005, Code of Practice for Information Security Management*

[12] ISACA (2007). *CObIT 4.1 – Control Objectives*. IT Governance Institute.

[13] ISACA (2007). *CObIT 4.1 – Framework*. IT Governance Institute.

[14] ISACA (2009). *The Risk IT Framework – Practitioner Guide*. IT Governance Institute.

[15] ISACA (2009). *The Risk IT Framework*. IT Governance Institute.

[17] ITENAS (2008). *Statuta Institut Teknologi Nasional Tahun 2008*.

[19] King, Jack L., 2001, *Operational Risk : Measurement and Modeling,* United Kingdom: Wiley, Chichester.

[22] Williams, Graham. (2007). *Management Of Risk: Guidance for Practitioners 3rd Edition*. The Cabinet Office.

[24] Project Management Institute (2008). *A Guide to the Project Management Body of Knowledge (PMBOK Guide) 4th Edition*. Project Management Institute, Inc.

[25] Stoneburner, Gary; Gougen, Alice & Feringa, Alexis (2002). *Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology.