USULAN KERANGKA MANAJEMEN RESIKO IMPLEMENTASI TEKNOLOGI BARU DALAM MENDUKUNG AKTIVITAS BISNIS PERUSAHAAN TELEKOMUNIKASI

Yohanes Suprapto
Magister Informatika, Sekolah Teknik Elektro dan Informatika (STEI), Institut Teknologi Bandung
Jl. Ganesha No. 10 Bandung 40132
Telp. (022) 2502260, Faks. (022) 2534222
E-mail: yohanes.suprapto@gmail.com

ABSTRAK
Penerapan teknologi baru dalam perusahaan seringkali bermanfaat dalam pengembangan bisnis perusahaan. Hal ini namun juga tidak jarang menimbulkan masalah yang bervariasi. Kegagalan atas penerapan teknologi baru pada umumnya disebabkan kurangnya analisis resiko terhadap pengimplementasian teknologi baru untuk mendukung kinerja bisnis perusahaan. Oleh sebab itu, resiko harus dikelola dengan baik agar dapat diminimalkan potensi kerugian yang ditimbulkan akibat terjadinya resiko tersebut. Terkait dengan penggunaan teknologi baru, aktivitas manajemen resiko akan mengurangi dampak kerugian atas pemanfaatan teknologi baru yang pada akhirnya akan mengakibatkan tidak terganggunya kinerja bisnis perusahaan. Hal ini menjadi sangat penting khususnya bagi perusahaan yang memanfaatkan teknologi sebagai komponen utama pada aktivitas bisnisnya seperti pada perusahaan telekomunikasi. Makalah ini memberikan usulan kerangka yang berisi tahapan-tahapan aktivitas manajemen resiko yang dapat dilakukan terhadap pemanfaatan teknologi baru dalam rangka mendukung aktivitas bisnis pada perusahaan telekomunikasi.

Kata Kunci: manajemen, resiko, teknologi, baru, perusahaan, telekomunikasi

1. PENDAHULUAN

Dalam mendukung kegiatan bisnisnya, sebuah perusahaan tentu tidak lepas dari teknologi yang digunakannya. Teknologi adalah semua perangkat keras dan lunak yang digunakan untuk membantu perusahaan melakukan aktivitas bisnisnya. Tujuan pemanfaatan teknologi informasi pada perusahaan adalah untuk mempermudah kinerja perusahaan dan meningkatkan hasil produksi perusahaan yang diharapkan akan didukung dengan penerapan berbagai teknologi yang ada pada perusahaan.

Penerapan teknologi baru seringkali menjadi tren dimanfaatkan di kalangan perusahaan khususnya perusahaan dengan banyak pesaing. Pemanfaatan teknologi baru ini seringkali dimaksudkan oleh perusahaan untuk mendapatkan daya tarik tersendiri maupun untuk dalam kaitannya dengan menempatkan pada persaingan bisnis dengan perusahaan-perusahaan lainnya. Dalam kaitannya dengan keputusan perusahaan menggunakan teknologi baru terdapat resiko-resiko yang ditimbukan. Resiko dan ketidakpastian mencirikan kondisi dimana sebenarnya hasil untuk peristiwa tertentu atau kegiatan cenderung menyimpang dari estimasi atau nilai prediksi. (Raftery, 1994)

Pada dasarnya, resiko dapat dikelola dengan pola manajemen resiko yang baik. Pentingnya pengelolaan resiko bagi perusahaan adalah perusahaan dapat mengurangi dampak daripada resiko atau mengurangi resiko tersebut sehingga dampak dari kerugian yang ditimbulkan atas resiko tersebut dapat dikurangi ataupun bahkan dapat dihilangkan. Pengelolaan resiko atas teknologi akan menjadi sebuah hal yang sangat penting bagi perusahaan, khususnya pada perusahaan yang menggunakan teknologi sebagai bagian/komponen utama pada kegiatan utama bisnisnya seperti pada perusahaan telekomunikasi.

Banyak *framework* aplikasi yang dapat dimanfaatkan oleh perusahaan dalam melakukan manajemen resiko terkait dengan pemanfaatan teknologi baru pada perusahaan. Pada prinsipnya, dengan penggunaan *framework* aplikasi ini akan mempermudah proses manajemen resiko yang dilakukan oleh perusahaan.

2. PERUSAHAAN TELEKOMUNIKASI

Perusahaan telekomunikasi merupakan perusahaan yang mendasarkan basis layanannya yaitu memberikan layanan kepada konsumennya dengan layanan-layanan berbasis telekomunikasi yang ditawarkan. Pada umumnya, sebuah perusahaan telekomunikasi dapat dibedakan menjadi perusahaan penyedia jasa layanan telekomunikasi bergerak (seluler), perusahaan penyedia jasa layanan telekomunikasi *fixed line* dan perusahaan jasa penyedia layanan telekomunikasi radio dan televisi serta berbasis internet.

Karakteristik perusahaan merupakan ciri khas yang dimiliki oleh perusahaan dalam melakukan kegiatannya yang umumnya berbeda antara satu perusahaan dan lainnya. Pada prinsipnya, pemanfaatan teknologi pada perusahaan telekomunikasi menjadi sebuah faktor yang paling penting dalam mendukung aktivitas bisnis utama perusahaan.

Karakteristik sebuah perusahaan telekomunikasi pada umumnya didasarkan atas kebijakan-kebijakan maupun aturan-aturan serta budaya dan perilaku yang terdapat pada perusahaan telekomunikasi tersebut. Secara umum mengenali karakteristik atas sebuah perusahaan telekomunikasi, dapat dilihat dengan mengenali perilaku manajemen dan budaya organisasi yang terdapat pada perusahaan tersebut. Dengan mengenali karakteristik perusahaan, langkah manajemen resiko yang tepat dapat dengan mudah ditentukan. Untuk teknologi baru dalam bentuk perangkat lunak, penggunaan proses *cleanroom* dapat digunakan menghasilkan produk perangkat lunak yang kurang rentan terhadap cacat, sehingga meningkatkan kualitas perangkat lunak dan kehandalan. (Walter, 1996)

3. KONSEP MANAJEMEN RESIKO

Secara umum, manajemen resiko merupakan sebuah tahapan atau langkah-langkah yang diterapkan untuk mengelola resiko yang ada agar dampak daripada resiko yang ditimbulkan dapat diminimalkan ataupun dapat dihilangkan. Manajemen resiko, berikutnya, adalah proses dimana organisasi upaya untuk membatasi efek dari resiko spekulatif. (Adler *et al.,* 1999) Manajemen resiko secara umum dilakukan melalui 4 tahapan yaitu *risk identification, risk assesment, risk mitigation* dan *risk evaluation*. *Risk identification* merupakan tahapan identifikasi resiko, *risk assesment* merupakan tahapan penilaian atas resiko-resiko yang ada, *risk mitigation* merupakan aktivitas mitigasi atau pengurangan resiko dan *risk evaluation* yang pada prinsipnya merupakan tahapan evaluasi atas kesesuaian pola manajemen resiko yang diterapkan. (Stoneburner *et al.*, 2002)

- Proses Identifikasi Resiko (*Risk Identification*)

  Proses identifikasi resiko pada prinsipnya adalah melakukan pengidentifikasian atas resiko yaitu apakah terdapat resiko pada kegiatan yang dilakukan dan bagaimana hal tersebut dapat diklasifikasikan.
- Proses Penilaian Resiko (*Risk Assesment*)

  Terdapat sembilan langkah dalam proses penilaian resiko yaitu :
  1. Melakukan karakterisasi sistem.
  2. Identifikasi ancaman yang mungkin menyerang kelemahan pada sistem.
  3. Identifikasi kekurangan atau kelemahan (*vulnerability*) pada prosedur keamanan, desain, implementasi, dan internal kontrol terhadap sistem sehingga menghasilkan pelanggaran terhadap kebijakan keamanan sistem.
  4. Menganalisa kontrol-kontrol yang telah diimplementasikan atau direncanakan untuk diimplementasikan.
  5. Penentuan kecenderungan (*likelihood*) dari kejadian.
  6. Analisa dampak yang kurang baik.
  7. Penentuan *level* (tingkat) resiko.
  8. Rekomendasi - rekomendasi untuk mengurangi level resiko sistem TI dan data sehingga mencapai *level* (tingkat) yang dapat diterima.
  9. Dokumentasi hasil dalam bentuk laporan.
- Proses Mitigasi Resiko (*Risk Mitigation*)

  Proses mitigasi resiko merupakan strategi untuk mengurangi timbulnya atau terjadinya resiko dengan *risk assumption*, *risk avoidance* atau pencegahan terjadinya resiko, *risk limitation* atau menerapkan batasan atas resiko dan *risk transference* atau pentransferan resiko. Secara ringkas, proses mitigasi resiko digambarkan melalui tahapan-tahapan berikut:
  1. Memprioritaskan aksi / tindakan.
  2. Evaluasi terhadap kontrol yang direkomendasikan.
  3. Melakukan *cost-benefit analysis*.
  4. Memilih kontrol.
  5. Memberikan tanggung jawab.
  6. Mengembangkan rencana implementasi *safeguard*.
  7. Mengimplementasikan kontrol yang dipilih.
- Proses Evaluasi Resiko (*Risk Evaluation*)

  Proses yang dilakukan adalah mengevaluasi kesesuaian atas pola manajemen resiko yang telah dilakukan apakah telah sesuai atau belum. Selain itu, juga dilakukan kembali proses *risk assesment* untuk memastikan keberadaan daripada resiko yang telah maupun yang belum teridentifikasi sebelumnya.

4. KERANGKA MANAJEMEN RESIKO IMPLEMENTASI TEKNOLOGI BARU PERUSAHAAN TELEKOMUNIKASI

Dalam pemanfaatan teknologi baru, proses manajemen resiko menjadi sangat penting khususnya pada perusahaan yang mendasarkan kegiatan bisnis utamanya berbasis/dengan menggunakan teknologi seperti pada perusahaan telekomunikasi agar resiko atas implementasi atau penggunaan teknologi baru dapat dikurangi/diminimalkan sehingga kinerja perusahaan akan tidak terhambat dan hasil produksi dan kualitas layanan yang diberikan akan tetap stabil dan mengalami peningkatan. Resiko adalah segala hal yang berdampak bagi organisasi dalam mencapai tujuan-tujuannya. (Maulana dan Supangkat, 2006)

Pada prinsipnya sebuah kerangka kerja merupakan urutan kumpulan pengetahuan pola pikir daripada sebuah pengembangan proses dan langkah yang diterapkan terkait dengan sebuah bidang atau domain pengetahuan tertentu. Sebuah kerangka kerja dapat berisi model-model yang dianggap representatif untuk diterapkan dalam menangani kasus tertentu. Usulan kerangka kerja yang dibuat tentu perlu memperhatikan kesesuaian dengan bidang yang dimaksudkan untuk diteliti.

Kerangka manajemen resiko pada penerapan teknologi baru yang digunakan pada perusahaan telekomunikasi secara garis besar dapat digambarkan terdiri dari tahapan-tahapan aktivitas:

1. Identifikasi strategi bisnis perusahaan telekomunikasi dalam kaitannya dengan teknologi baru yang akan diterapkan dan posisi atas teknologi baru yang akan diterapkan serta perencanaan strategis perusahaan terhadap pemanfaatan teknologi baru yang diterapkan.
2. Identifikasi atas tujuan penerapan teknologi baru yang akan digunakan dan melakukan proses identifikasi resiko.
3. Melakukan tahapan penilaian atas resiko atau tahapan-tahapan *risk assesment* yang ada.
4. Merencanakan manajemen resiko dengan mencoba melakukan pengembangan atas strategi-strategi proteksi yang mungkin diterapkan dalam menangani resiko yang mungkin ditimbulkan.
5. Melakukan tahapan manajemen resiko yaitu tahapan *risk mitigation* atau pengurangan atas resiko dengan tahapan-tahapan yang ada.
6. Melaporkan resiko-resiko yang ada berdasarkan atas informasi yang diperoleh dari tahapan-tahapan sebelumnya.
7. Melakukan prediksi atas resiko (*risk prediction*) berdasarkan atas tahapan-tahapan yang telah dilakukan sebelumnya.
8. Melakukan tahapan *risk evaluation* yaitu evaluasi atas proses manajemen resiko yang dilakukan apakah sudah sesuai dan dilakukan kembali tahapan risk assesment untuk memastikan keberadaan semua resiko yang ada yaitu resiko yang telah dan belum teridentifikasi.

1. Identifikasi strategi bisnis perusahaan telekomunikasi dalam kaitannya dengan teknologi baru yang akan diterapkan dan posisi teknologi baru yang akan diterapkan serta perencanaan strategis perusahaan terhadap pemanfaatan teknologi baru yang diterapkan.

   Identifikasi atas strategi bisnis perusahaan telekomunikasi dalam kaitannya dengan teknologi baru yang akan diterapkan diperlukan sebagai langkah awal untuk masuk pada manajemen resiko atas pemanfaatan teknologi baru pada perusahaan telekomunikasi tersebut. Dengan melakukan identifikasi strategi bisnis perusahaan, maka akan dapat diketahui apakah teknologi baru yang akan ditetapkan telah sejalan dengan strategi bisnis perusahaan dalam kaitannya dengan pencapaian tujuan strategis (visi, misi ataupun sasaran) perusahaan.

   Melalui identifikasi posisi, maka posisi dari teknologi baru dalam perusahaan dapat teridentifikasi dan perencanaan strategis yang mengarah pada tujuan pencapaian perusahaan akan pemanfaatan teknologi baru akan juga teridentifikasi sehingga diharapkan akan mengarahkan kita pada sebuah pola manajemen resiko yang terarah dan benar sehingga pola manajemen resiko yang dihasilkan akan menjadi bermanfaat bagi perusahaan.
2. Identifikasi atas tujuan penerapan teknologi baru yang akan digunakan dan melakukan proses identifikasi resiko yang timbul atas tindakan yang dilakukan.

   Hal ini juga sangat perlu untuk dilakukan untuk mempermudah memahami secara keseluruhan tentang sistem yang digunakan dan karakteristiknya yang akan dicoba untuk diidentifikasikan pada awal tahapan *risk assesment* (penilaian atas resiko). Proses Identifikasi Resiko (*Risk Identification*)

   Proses identifikasi resiko dilakukan dengan melakukan pengidentifikasian atas resiko yaitu apakah terdapat resiko pada kegiatan yang dilakukan dalam hal ini adalah pada kegiatan penerapan atau pemanfaatan teknologi baru untuk mendukung aktivitas bisnis suatu perusahaan telekomunikasi dan bagaimana hal tersebut dapat diklasifikasikan.
3. Melakukan tahapan identifikasi dan analisis resiko (penilaian atas resiko) melalui tahapan-tahapan *risk assesment* yang ada:
   1. Melakukan karakterisasi sistem.

      Hal ini berbicara tentang karakteristik sistem dari teknologi baru yang akan diterapkan di perusahaan telekomunikasi tersebut meliputi perangkat keras, perangkat lunak dan antar muka pengguna secara detail bahkan termasuk data dan informasi yang terdapat di dalamnya dan orang-orang yang mendukung atau menggunakan teknologi baru ini, arsitektur keamanan dan topologi jaringan sistem teknologi baru yang digunakan. *Output* atau hasil yang diperoleh adalah karakteristik lengkap dari teknologi baru yang digunakan.
   2. Identifikasi ancaman yang mungkin menyerang sistem yang dapat berasal dari alam, manusia dan lingkungan.

      Hal ini merupakan hal utama untuk perusahaan dapat memanajemen resiko dengan baik. Ancaman pada penggunaan teknologi baru titik beratnya adalah pada manusia, alam dan lingkungan. Identifikasi dilakukan dengan membuat tabel *potential threat* yang berisi sumber ancaman, tindakan aksi dan motivasi daripada ancaman yang ditimbulkan.

      Ancaman dari alam dapat berupa berbagai bentuk bencana alam yang terjadi, ancaman dari manusia pada umumnya dapat berasal dari dalam lingkungan perusahaan yaitu petugas yang melakukan kesalahan, dan dalam kaitan dengan pemanfaatan teknologi

baru ancaman dapat berupa ketidakpuasan di kalangan karyawan pada perusahaan akan pemanfaatan teknologi yang pada umumnya terjadi karena telah nyaman menggunakan teknologi lama atau bahkan dari penjahat jaringan, pencuri, perampok dan teroris. Ancaman yang berasal dari lingkungan juga harus diperhatikan terdiri atas ancaman demo dari masyarakat sekitar (*society*) atau protes sosial dan lain sebagainya.

3. Identifikasi *vulnerability* pada sistem.

   Proses identifikasi ini melihat pada identifikasi kelemahan pada prosedur keamanan, desain, implementasi, dan internal kontrol terhadap sistem sehingga menghasilkan pelanggaran terhadap kebijakan keamanan sistem. Identifikasi ini dapat menghasilkan *list of vulnerability* pada tiap aspek yang diidentifikasikan yang berguna dalam proses manajemen resiko dari sistem teknologi yang digunakan.
4. Menganalisa kontrol - kontrol yang telah diimplementasikan atau direncanakan untuk diimplementasikan oleh organisasi untuk mengurangi atau menghilangkan kecenderungan (kemungkinan) dari suatu ancaman menyerang sistem yang *vulnerable*.

   Hal ini mengandung pengertian bahwa perusahaan telekomunikasi memberikan pengendalian atas kecenderungan terjadi ancaman terhadap sistem/teknologi baru yang *vulnerable*, dimana ada kontrol-kontrol dan mekanisme pengendalian yang dibuat dan diidentifikasikan. Tahapan ini mengacu pada setiap *vulnerability* yang telah diidentifikasikan sebelumnya.
5. Penentuan kecenderungan (*likelihood*) dari kejadian bertujuan untuk memperoleh penilaian terhadap keseluruhan kecenderungan yang mengindikasikan kemungkinan potensi kerentanan diserang oleh lingkungan-lingkungan ancaman yang ada.

   Pada langkah ini ditentukan kecenderungan yang ada terhadap kejadian untuk mngindikasikan kemungkinan potensi kerentanan diserang oleh lingkungan ancaman yang ada. Dalam hal ini faktor penentuan kecenderungan melihat pada faktor ancaman dan potensi kerentanan yang memiliki kemungkinan untuk mndapatkan serangan dari lingkungan ancaman yang ada, dan ditentukan kecenderungan atas hal tersebut. Output dari tahap ini adalah diperolehnya kecenderungan (*likelihood*) dari kejadian.
6. Analisa dampak yang kurang baik yang dihasilkan dari suksesnya ancaman menyerang *vulnerability* seperti *loss of integrity*, *loss of availability*, dan *loss of confidentiality*.

   Pengukuran dampak dari resiko TI dapat dilakukan baik secara kualitatif maupun kuantitatif. Dampak tersebut dapat diklasifikasikan menjadi 3 bagian yaitu : *high*, *medium* dan *low*.
7. Penentuan *level* (tingkat) resiko.

   Penentuan *level* resiko dari Sistem TI yang merupakan pasangan ancaman/ *vulnerability* merupakan suatu fungsi :
   - Kecenderungan suatu sumber ancaman menyerang *vulnerability* dari sistem teknologi baru ini.
   - Besaran dampak yang akan terjadi jika sumber ancaman sukses menyerang *vulnerability* dari sistem.
   - Terpenuhinya perencanaan kontrol keamanan yang ada untuk mengurangi dan menghilangkan resiko.
8. Rekomendasi - rekomendasi untuk mengurangi level resiko sistem dan data sehingga mencapai level yang dapat diterima.

   Rekomendasi dibuat berdasarkan atas identifikasi-identifikasi pada tahapan-tahapan yang telah dilakukan sebelumnya sehingga mencapai *level* yang dapat diterima.
9. Dokumentasi hasil dalam bentuk laporan.

   Setiap tahapan hasil daripada proses penilaian resiko termuat dan tercantum secara jelas dan sistematis dalam sebuah dokumentasi berbentuk laporan, sehingga dapat digunakan untuk keperluan evaluasi atas tahapan-tahapan yang telah dilakukan oleh perusahaan dikemudian hari.

4. Merencanakan manajemen resiko dengan mencoba melakukan pengembangan atas strategi-strategi proteksi yang mungkin diterapkan dalam menangani resiko yang mungkin ditimbulkan.

   Strategi-strategi proteksi yang mungkin untuk diterapkan dapat diterapkan dalam menangani resiko yang mungkin ditimbulkan.
5. Melakukan tahapan-tahapan mitigasi resiko:
   1. Memprioritaskan aksi.

      Berdasarkan *level* (tingkat) resiko yang ditampilkan dari hasil penilaian resiko, implementasi dari aksi diprioritaskan. Pada langkah ini secara detail dihitung bobot aksi atau tindakan sehingga pada keluaran dari langkah pertama dalam tahap mitigasi resiko ini adalah peringkat aksi-aksi mulai dari peringkat tinggi hingga rendah.
   2. Evaluasi terhadap kontrol yang direkomendasikan.

      Pada langkah ini, kelayakan (seperti kompatibilitas, penerimaan dari *user*) dan efektifitas (seperti tingkat proteksi dan level dari pengurangan resiko) dari pilihan-pilihan kontrol yang direkomendasikan dianalisa

dengan tujuan untuk meminimalkan resiko. Keluaran dari langkah kedua adalah berupa daftar kontrol-kontrol yang layak untuk diterapkan.

3. Melakukan *cost-benefit analysis* (analisa biaya dan keuntungan).

Suatu *cost-benefit analysis* dilakukan untuk menggambarkan biaya dan keuntungan ketika kita memilih untuk mengimplementasikan maupun tidak mengimplementasikan kontrol - kontrol tersebut.

4. Memilih kontrol.

Berdasarkan atas hasil *cost-benefit analysis*, manajemen menentukan kontrol dengan biaya paling efektif untuk mengurangi resiko yang ditimbulkan terhadap misi organisasi.

5. Memberikan tanggung jawab.

Dalam hal ini dibuat daftar personil yang bertanggungjawab dalam mengimplementasikan kontrol yang diidentifikasi.

6. Mengembangkan rencana implementasi *safeguard*.

Implementasi *safeguard* sekurang-kurangnya meliputi informasi tentang resiko (pasangan *vulnerability*/ ancaman) dan tingkat resiko (hasil dari laporan penilaian resiko), kontrol yang direkomendasikan (hasil dari laporan penilaian resiko, aksi-aksi yang diprioritaskan (dengan prioritas yang diberikan terhadap pilihan *level* resiko tinggi atau amat tinggi), melakukan pemilihan atas kontrol yang telah direncanakan yang ditentukan berdasarkan pada kelayakan, efektifitas, keuntungan terhadap organisasi dan biaya, sumberdaya yang dibutuhkan didalam melakukan implementasi pada pilihan kontrol yang telah direncanakan, membuat daftar personil yang bertanggung jawab berikut dengan tanggal dimulainya implementasi, tanggal target penyelesaian untuk implementasi dan kebutuhan untuk perawatan (*maintainance*).

7. Mengimplementasikan kontrol yang dipilih.

Pada kondisi tertentu, kontrol yang dipilih akan menurunkan resiko akan tetapi tidak dapat menghilangkan resiko. *Output* dari langkah ketujuh adalah sisa resiko (*residual risk*).

6. Melaporkan resiko-resiko yang diperoleh (*risk reporting*) berdasarkan atas resiko-resiko yang didapatkan pada tahap sebelumnya.

Resiko-resiko yang diperoleh dari tahapan-tahapan sebelumnya (*risk identification, risk assesment* dan *risk mitigation*) dilaporkan.

7. Memprediksi resiko-resiko yang dapat muncul pada masa mendatang (melakukan *risk prediction*).

Prediksi resiko dilakukan berdasarkan atas tahapan-tahapan yang telah dilakukan sebelumnya (*risk identification, risk assesment* dan *risk mitigation*). Prediksi yang dimaksudkan mencakup prediksi menggunakan sejarah dan pengetahuan dari resiko-resiko yang telah diidentifikasikan sebelumnya.

8. Melakukan tahapan *risk evaluation* yaitu evaluasi atas proses manajemen resiko yang dilakukan apakah sudah sesuai dan dilakukan kembali tahapan *risk assesment* untuk memastikan keberadaan resiko yang telah dan belum teridentifikasi.

Evaluasi atas resiko dilakukan dengan memeriksa kembali relevan atau tidak proses manajemen resiko yang dilakukan dengan apa yang ingin dicapai, kesesuaian langkah dalam proses manajemen resiko dan memastikan keberadaan resiko yang telah dan belum teridentifikasi dengan kembali melakukan tahapan-tahapan *risk assesment*.

5. KESIMPULAN

Penerapan manajemen resiko sangat diperlukan oleh perusahaan untuk dapat mengurangi kerugian yang ditimbulkan atas resiko-resiko yang ada pada sebuah tindakan yang dilakukan, khususnya pada perusahaan yang mendasarkan kegiatan utamanya pada teknologi seperti pada perusahaan telekomunikasi. Untuk itulah diperlukan sebuah kerangka manajemen resiko yang sistematis untuk sebuah perusahaan telekomunikasi dapat melakukan manajemen resiko yang terarah. Melalui delapan tahapan aktivitas dalam kerangka yang diusulkan, diharapkan proses manajemen resiko pada sebuah perusahaan telekomunikasi dapat berjalan dengan baik, terarah dan tujuan yang diharapkan dapat berhasil dengan baik, sehingga resiko yang ada dapat dikurangi dan diantisipasi dengan baik.

PUSTAKA

Adler, T., Leonard, J. and Nordgen, R. (1999). "Improving risk management: moving from risk elimination to risk avoidance", *Information and Software Technology*, 41, 29-34.

Maulana, M. dan Supangkat, S. (2006). "Pemodelan Framework Manajemen Resiko Teknologi Informasi untuk Perusahaan Negara Berkembang", *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia, 3-4 Mei 2006, Institut Teknologi Bandung*.

Raftery, J. (1994). *Risk Analysis in Project Management*. First Edition. UK: E & FN Spon.

Stoneburner, G., Goguen, A. and Feringa, A. (2002). "Risk Management Guide for Information Technology System", *Recommedation of National Institute of Standards and Technology, Special Publication 800-30*.

Walter, D. (1996). *Software Engineering Risk Management*. USA: IEEE Computer Society Press.

Hofstede, G. (1997). *Cultures and Organizations: Software of the Mind*. New York: McGraw-Hill.

Katz, J. E., dan Aspden, P. (1997). A nation of strangers. *Communications of the ACM, 40*(12), 81-86.