# PERAN KEBIJAKAN PENGAMANAN INFORMASI DALAM MANAJEMEN RISIKO ATAS INFORMASI



**Oleh:**
**Michael Iskandar**

**FAKULTAS EKONOMI**
**UNIVERSITAS KATOLIK PARAHYANGAN**
**BANDUNG**
**2006**

# Peran Kebijakan Pengamanan Informasi Dalam Manajemen Risiko Atas Informasi

Michael Iskandar

*Fakultas Ekonomi*
*Universitas Katolik Parahyangan*
Jalan Ciumbuleuit 94 Gedung 9 Bandung 40141

*E-mail: mike78@home.unpar.ac.id*

**Abstrak**

Risiko yang dihadapi oleh sumber daya informasi perusahaan harus dikelola dalam upaya meminimalkan kemungkinan risiko tersebut menjadi kenyataan. Hal ini dapat dilakukan dengan melakukan manajemen risiko atas informasi, yang dilakukan dalam empat tahap, yaitu: identifikasi pihak yang mengancam, definisikan risiko yang dihadapi, susun Kebijakan Pengamanan Informasi, serta implementasikan *controls* yang dibutuhkan.

Jika seseorang berpikir tentang *controls* sebagai aspek pengamanan informasi dan sistem informasi perusahaan, maka yang sering terbayang adalah *technical controls* yang terkait, misalnya saja: firewall dan enkripsi. Padahal di luar *technical controls* tersebut juga dikenal perangkat-perangkat pengendali yang lain, yaitu *formal controls* dan *informal controls*. Semuanya ini tentu perlu diatur, dan pengaturan itu dimulai dari penyusunan Kebijakan Pengamanan Informasi yang sesuai.

Dalam tulisan ini akan dibahas mengenai bentuk-bentuk manajemen risiko, metodologi manajemen risiko atas informasi, hakekat dan cara penyusunan Kebijakan Pengamanan Informasi, yang kemudian dianalisa sehingga diperoleh kesimpulan mengenai peran dari Kebijakan Pengamanan Informasi dalam manajemen risiko atas informasi.

***Kata kunci:*** *Manajemen Risiko, Kebijakan Pengamanan Informasi, Formal Control, Informal Control, Technical Control*

## 1. Pendahuluan

Informasi di perusahaan-perusahaan masa kini telah diakui sebagai sebuah sumber daya yang penting, sama pentingnya dengan sumber daya manusia, uang, mesin dan bahan baku, serta pasar. Oleh karena itu sistem informasi perusahaan juga serta merta menjadi sesuatu yang sangat penting pula. Sedemikian pentingnya informasi dan sistem informasi itu, sehingga kebanyakan perusahaan-perusahaan mengakui bahwa seandainya terjadi sesuatu yang buruk atas informasi atau sistem informasi mereka, maka dapat berdampak besar atas kinerja dan profitabilitas perusahaan. Oleh karena itu risiko yang dihadapi oleh sumber daya informasi perusahaan harus dikelola dalam upaya meminimalkan kemungkinan terjadinya risiko tersebut, serta meminimalkan pengaruh dari risiko tersebut seandainya terjadi juga.

## 2. Pengertian Manajemen Risiko

Manajemen risiko (*risk management*) adalah setiap upaya yang dilakukan perusahaan untuk mengantisipasi, mencegah, ataupun meminimalkan kerugian yang harus ditanggung seandainya suatu risiko menjadi kenyataan. Pada dasarnya ada dua pendekatan besar atas manajemen risiko: (Handout Pelatihan Telkom, h. 11)

a. Manajemen risiko sebagai sebuah proses yang melindungi pendapatan dan kekayaan perusahaan atau individu;
b. Manajemen risiko sebagai sebuah proses identifikasi, penilaian, dan pengawasan terhadap risiko-risiko yang merupakan ancaman.

Dalam konteks (a) di atas, maka manajemen risiko memiliki konsekuensi bahwa pendapatan atau kekayaan milik perusahaan atau individu tidak akan hilang apabila suatu risiko menjadi kenyataan. Contoh yang paling sederhana adalah penggunaan jasa asuransi. Sebuah perusahaan yang membeli polis asuransi kebakaran telah melakukan manajemen risiko, yaitu seandainya terjadi kebakaran di perusahaan itu, maka kerugian yang dialami tidak perlu ditanggung sendiri (dengan dampak negatif pada kekayaan perusahaan, bahkan kelangsungan hidup perusahaan), melainkan sampai batas tertentu kerugian itu telah dialihtanggungkan kepada perusahaan asuransi.

Pada pendekatan yang ke-dua, manajemen risiko diartikan sebagai semua kegiatan untuk mengidentifikasi, menilai, dan mengawasi risiko yang dihadapi

perusahaan. Maksudnya adalah untuk sedapat mungkin mencegah suatu risiko menjadi kenyataan. Contoh dari pendekatan yang terakhir ini adalah pendekatan *software engineering risk management* yang dijelaskan oleh Karolak, di mana beliau menganjurkan agar seluruh siklus rekayasa perangkat lunak dilaksanakan menggunakan pendekatan *Just-in-Time*, dengan tujuan agar perangkat lunak yang dikembangkan tidak *over schedule* ataupun *over budget*. (Karolak, 1996: h. 15-20)
Di sini tentu saja yang diharapkan dari manajemen risiko adalah bahwa risiko tersebut tidak akan terjadi sama sekali, bukan bahwa risiko itu dapat dialihtanggungkan kepada pihak lain seperti pada pendekatan pertama.

Dengan kata-kata yang lebih sederhana, pendekatan pertama memiliki semangat, "seandainya risiko menjadi kenyataan, kita sudah siap menghadapinya.", sedangkan pendekatan kedua adalah "risiko diusahakan tidak terjadi, karena kita sudah mengambil langkah-langkah pencegahan dan pengawasan yang sesuai." Terlihat jelas adanya nuansa yang berbeda dalam menghadapi risiko di antara kedua pendekatan tersebut.

### 3. Manajemen Risiko atas Informasi

Yang menjadi pertanyaan adalah, bagaimanakah manajemen risiko dilakukan atas informasi? McLeod dan Schell menjelaskan bahwa manajemen risiko atas informasi mengikuti metodologi sebagai berikut: (McLeod & Schell, 2004: h. 210-211)

a. Identify the threats
b. Define the risks
c. Establish Information Security Policy
d. Implement the controls

### 3.1. Mengidentifikasi Ancaman

Pada langkah pertama, *identify the threats*, maka manajer informasi harus mengidentifikasi pihak-pihak mana saja yang dapat dianggap sebagai ancaman terhadap informasi perusahaan. Dalam hal ini ada dua pihak yang bisa menjadi ancaman, yaitu: pihak internal atau orang-orang yang termasuk *legitimate users*

(misalnya: karyawan perusahaan), serta pihak eksternal atau orang-orang yang termasuk *illegitimate users* (misalnya: hackers). Selain itu juga harus dibedakan antara ancaman yang disengaja (*deliberate*) dan ancaman yang tidak disengaja (*accidental*). Contoh dari ancaman yang disengaja adalah seseorang yang sengaja melakukan *hacking* untuk bisa memperoleh informasi tertentu yang bersifat rahasia, sedangkan contoh dari ancaman yang tidak disengaja adalah seorang pengguna yang secara tidak sengaja membuka file yang sebenarnya tidak boleh dia baca.

### 3.2. Aktiva Informasi

Langkah kedua disebut oleh McLeod dan Schell sebagai *define the risks*. Dalam hal ini kegiatan-kegiatan yang harus dilakukan manajer informasi adalah, pertama-tama: mengidentifikasi aktiva-aktiva informasi yang menghadapi risiko. Kemudian, jenis risiko yang mungkin dihadapi oleh setiap aktiva tersebut.

Tipton dan Krause mendefinisikan aktiva informasi (*information asset*) sebagai seluruh informasi yang harus dimiliki sebuah organisasi agar dapat menjalankan usahanya.(Tipton & Krause, 2006) Untuk dapat memberikan nilai atas suatu aktiva informasi (misalnya: informasi utang dagang, informasi stok barang, informasi tentang gaji), maka perlu dilakukan penilaian atas beberapa elemen yang mendasari aktiva tersebut, yaitu:

- Biaya yang harus dikeluarkan seandainya informasi itu hilang dan harus diganti.
- Biaya yang harus dikeluarkan seandainya perangkat lunak pendukung informasi itu harus diganti.
- Biaya/kerugian yang timbul akibat hilangnya kerahasiaan informasi tersebut (*loss of confidentiality*)
- Biaya/kerugian yang timbul akibat hilangnya ketersediaan informasi tersebut (*loss of availability*)
- Biaya/kerugian yang timbul akibat hilangnya integritas informasi tersebut (*loss of integrity*)

Meskipun biaya-biaya itu dapat diperkirakan, namun untuk menghitung total kerugian, belum tentu kelima komponen biaya itu dapat langsung dijumlah secara

sederhana. Sejumlah metrik lain telah disiapkan untuk melakukan perkiraan dengan cara yang lebih dapat dipertanggungjawabkan.

### 3.2.1. Metrik Risiko Aktiva Informasi

Tipton dan Krause menyebutkan sejumlah metrik yang telah dikembangkan untuk melakukan penilaian yang lebih spesifik atas risiko yang dihadapi aktiva informasi tadi. Pertama-tama perlu ditentukan *Exposure Factor* (EF), yaitu sebuah nilai persentase antara 0% hingga 100% yang menunjukkan seberapa besarnya nilai aktiva akan hilang seandainya suatu ancaman terjadi. Apabila EF telah ditentukan, maka dapat dihitung *Single Loss Expectancy* (SLE) dengan rumus sebagai berikut:

Single Loss Expectancy = Nilai Aktiva × Exposure Factor..... (1)

Setelah SLE diketahui, maka perlu juga ditentukan *Annualized Rate of Occurrence* (ARO), yaitu nilai perkiraan seberapa seringnya suatu risiko akan menjadi kenyataan dalam kurun waktu setahun. Misalnya, jika diperkirakan bahwa suatu risiko akan terjadi 30 kali dalam setahun, maka AROnya adalah 30; jika diperkirakan bahwa suatu risiko akan terjadi hanya satu kali dalam 10 tahun, maka AROnya adalah 0,1. Secara teoritis, ARO memiliki rentang dari 0,0 (tidak akan pernah terjadi) hingga bilangan positif tak terhingga (selalu terjadi). Sebagai contoh, apabila sebuah perusahaan memiliki 10.000 pekerja, dan diperkirakan bahwa setiap pekerja, secara sengaja ataupun tidak disengaja, memasukkan satu virus komputer ke dalam sistem informasi perusahaan setiap minggu, maka ARO atas risiko serangan virus komputer adalah 52 × 10.000 = 520.000. Sebuah nilai yang cukup mencengangkan, dan biasanya dapat mempengaruhi manajemen perusahaan untuk melakukan manajemen risiko atas sumber daya informasi secara sungguh-sungguh.

Perlu diperhatikan bahwa ARO tidak sama dengan probabilitas, yang memiliki rentang dari 0,0 hingga 1,0 saja. Probabilitas 0,0 berarti tidak mungkin terjadi (dalam hal ini artinya sama dengan ARO), tetapi 1,0 berarti pasti terjadi. Yang terakhir ini tidak sama dengan ARO, di mana 1,0 berarti perkiraan terjadinya ancaman adalah satu kali dalam setahun.

Apabila SLE dikalikan dengan ARO, maka kita akan memperoleh nilai *Annualized Loss Expectancy* (ALE) sebagai berikut:

ALE = Single Loss Expectancy × Annualized Rate of Occurrence.....(2)

Dengan menggunakan rumus-rumus di atas, maka manajer informasi dapat memperoleh nilai ALE untuk berbagai aktiva informasi, sehingga ia mendapat gambaran menyeluruh tentang skala prioritas aktiva informasi yang kritis perlu dilakukan manajemen risiko.

### 3.3. Mendefinisikan Jenis Risiko

Setelah mengidentifikasi pihak-pihak yang mengancam aktiva informasi, McLeod dan Schell menyebutkan bahwa langkah berikutnya adalah *define the risks* (mendefinisikan risiko). Jenis-jenis risiko yang dapat terjadi adalah:

- *Unauthorized disclosure and theft.* Yaitu penampilan informasi tanpa otorisasi, atau pencurian informasi. Misalnya, seorang karyawan perusahaan mengakses intranet perusahaan dan dapat melihat informasi rahasia tentang produk perusahaan yang akan dipasarkan bulan depan, padahal karyawan itu sebenarnya tidak boleh melihat informasi tersebut.
- *Unauthorized use.* Yaitu penggunaan informasi tanpa otorisasi, seperti misalnya seseorang yang menggunakan kartu kredit milik orang lain untuk melakukan pembelian barang.
- *Unauthorized destruction and Denial of Service.* Yaitu pengrusakan aktiva informasi, misalnya saja seseorang menghapus file tertentu padahal dia tidak memiliki hak untuk menghapus file tersebut. *Denial of service* terjadi apabila

seseorang dapat menyebabkan orang lain yang berhak menggunakan sistem informasi atau informasi tertentu, menjadi terhalang menggunakannya. Contohnya, seseorang mengubah password orang lain ke sistem informasi perusahaan, sehingga orang lain itu (yang berhak menggunakan sistem informasi) menjadi tidak bisa melakukan login.

- *Unauthorized modification.* Yaitu mengubah informasi tertentu tanpa otorisasi, misalnya seseorang mengubah data pribadi orang lain pada database perusahaan, padahal telah dibuat peraturan bahwa data pribadi seseorang hanya dapat diubah oleh orang yang bersangkutan.

Setelah menentukan jenis-jenis risiko yang dihadapi oleh masing-masing aset informasi, maka manajer juga harus mengkaji *level of impact* dan *vulnerabilities* dari aset informasi tersebut. McLeod dan Schell menggambarkannya menggunakan matriks sebagai berikut:

**Tabel 1: Matriks Level of Impact vs. Vulnerability**

| | **Severe Impact** | **Significant Impact** | **Minor Impact** |
|---|---|---|---|
| | Conduct Vulnerability Analysis | Conduct Vulnerability Analysis | Vulnerability analysis unnecessary |
| **High Vulnerability** | Must improve controls | Must improve controls | |
| **Medium Vulnerability** | Should improve controls | Should improve controls | |
| **Low Vulnerability** | Keep controls intact | Keep controls intact | |

(sumber: McLeod & Schell, h. 214)

Kondisi *severe impact* berarti bahwa seandainya risiko tersebut menjadi kenyataan maka perusahaan akan bangkrut; *significant impact* berarti bahwa seandainya risiko terjadi maka perusahaan akan mengalami kerugian yang besar, namun tidak akan sampai bangkrut; sedangkan *minor impact* adalah jenis risiko yang apabila terjadi akan mengganggu sesaat tetapi tidak terlalu besar pengaruhnya untuk jangka panjang.

Seperti yang terlihat pada matriks di atas, apabila sebuah risiko termasuk *severe* atau *significant impact* maka perlu dilakukan sebuah *vulnerability analysis*. Di dalam analisa ini dilakukan pengkajian, apakah untuk risiko tersebut aset informasi memiliki *high, medium,* atau *low vulnerability*. Berdasarkan hasil *vulnerability analysis* itu, manajer informasi dapat menentukan apakah perangkat pengendali (*control*) yang telah diterapkan perlu diperbaiki atau tidak.

### 3.4. Perangkat Pengendali (Control)

*Control* yang dimaksudkan di atas adalah segala macam perangkat yang digunakan perusahaan untuk mengawasi, mengendalikan dan mencegah terjadinya berbagai risiko yang telah diidentifikasikan tadi. *Control* terdiri atas tiga golongan besar yaitu,

- *Technical Control*, mencakup segala macam peralatan teknis untuk menjaga keamanan sistem, misalnya saja: *firewall, access control* (seperti *password* dan *biometrics*), dan enkripsi.
- *Formal Control*, mencakup berbagai peraturan-peraturan perusahaan yang secara langsung mengatur tata cara penggunaan informasi dan sistem informasi.
- *Informal Control*, mencakup berbagai pemikiran dan semangat yang diberlakukan di perusahaan yang secara tak langsung dapat mencegah terjadinya sejumlah risiko atas aset informasi. Contoh dari informal control adalah kode etik yang diberlakukan di perusahaan, visi dan misi perusahaan.

Dengan telah diselesaikannya *vulnerability analysis*, maka manajer informasi dapat melanjutkan ke tahap-tahap berikutnya yaitu menyusun kebijakan-kebijakan pengamanan informasi (*information security policy*), dan mengimplementasikan berbagai macam *controls* tadi.

Tulisan ini selanjutnya berfokus pada Kebijakan Pengamanan Informasi serta perannya dalam manajemen risiko atas informasi.

## 4. Hakekat dan Penyusunan Kebijakan Pengamanan Informasi

Seperti yang telah terlihat pada upabab 3.4. di atas, salah satu perangkat pengendali yang diperlukan perusahaan untuk melakukan manajemen risiko adalah

*formal control*, yaitu peraturan-peraturan yang mengatur tata cara penggunaan informasi dan sistem informasi oleh semua bagian yang terkait. Pada prakteknya, peraturan-peraturan ini adalah sama dengan, atau bersumber dari, Kebijakan Pengamanan Informasi (*Information Security Policy*).

Ada dua jenis Kebijakan Pengamanan Informasi, yaitu yang bersifat *Program-level* dan yang bersifat *Issue-specific.* Perbedaan di antara keduanya adalah dari hal yang diaturnya; kebijakan program-level adalah kebijakan yang mengatur suatu program sistem informasi secara umum, misalnya program *information security.* Sebaliknya kebijakan *issue-specific* adalah kebijakan yang mengatur hal tertentu yang sangat spesifik, misalnya kebijakan tentang penggunaan email di perusahaan. (Roback, 2002)

Bentuk dari Kebijakan Pengamanan Informasi ini sering sudah sangat detail, sehingga sudah merupakan peraturan tersendiri; namun ada pula kebijakan-kebijakan yang masih perlu dijabarkan ke dalam peraturan-peraturan pelaksanaan lagi. Misalnya, kebijakan tentang *password* di sebuah perusahaan mungkin saja sudah sangat detail, mencakup jenis-jenis *password* (system-level, user-level, dan lain-lain), hingga cara-cara membuat password yang baik ("pergunakan kombinasi huruf dan angka dan tanda baca"), serta pembuatan password yang dilarang ("tidak boleh menggunakan kata-kata yang tidak sopan atau menghina"). Di lain pihak, *risk assessment policy* dari perusahaan yang sama mungkin saja hanya menyebutkan bahwa Divisi Informasi perusahaan "memiliki hak dan kewajiban untuk melakukan *risk assessment* secara berkala", sedangkan tentang tata cara *risk assessment*-nya sendiri diatur dalam peraturan lain yang lebih spesifik.

Bagaimanapun, skema umum dari Kebijakan Pengamanan Informasi adalah sebagai berikut: (SANS, 2006)

a. Tujuan
b. Ruang Lingkup
c. Kebijakan
d. Sanksi
e. Definisi
f. Sejarah Revisi

Bagian pertama, yaitu *Tujuan*, mengungkapkan tujuan dari pengadaan kebijakan ini. Kemudian *Ruang Lingkup* menyebutkan apa saja yang diatur oleh kebijakan ini, serta pihak mana saja yang terpengaruh oleh kebijakan ini. Bagian *Kebijakan* menjelaskan tentang isi dari kebijakan itu sendiri, dan *Sanksi* menyebutkan secara umum sanksi apa yang akan dikenakan atas mereka yang terbukti melanggar kebijakan tersebut. Bagian *Definisi* menyebutkan sejumlah istilah yang dipergunakan dalam kebijakan beserta penjelasannya; tujuannya adalah agar tidak ada pihak yang di kemudian hari menyatakan salah memahami kebijakan karena menggunakan referensi yang berbeda. Bagian terakhir, *Sejarah Revisi*, adalah tempat untuk mencatat segala macam perubahan yang pernah terjadi atas kebijakan itu.

Perlu dicatat bahwa skema umum itu hanya berfungsi sebagai *guideline* dan bukan merupakan bentuk yang sudah baku. Misalnya, untuk kebijakan-kebijakan tertentu bisa saja dirasakan perlu untuk menambahkan bagian-bagian yang baru, dan mungkin saja untuk kebijakan-kebijakan yang lain beberapa bagian dapat dihilangkan.

### 4.1. Sebuah Contoh Kebijakan Pengamanan Informasi

Berikut adalah sebuah contoh Kebijakan Pengamanan Informasi atas penggunaan fasilitas email perusahaan tertentu, sebut saja "PT. X".

**Kebijakan Penggunaan Email PT. X**

**1.0. Tujuan**

Tujuan dari kebijakan ini adalah untuk mencegah rusaknya nama perusahaan PT. X di mata umum. Ketika sebuah email dikirim dari PT. X ke masyarakat luar, maka hal ini akan cenderung diartikan sebagai sebuah pernyataan resmi dari PT. X.

**2.0. Ruang Lingkup**

Kebijakan ini mencakup penggunaan email yang dikirim dari setiap alamat email PT. X dan berlaku bagi semua karyawan, pengecer, dan agen yang beroperasi atas nama PT. X.

**3.0. Kebijakan**

**3.1. Larangan Penggunaan**

Sistem email PT. X tidak boleh dipergunakan untuk pembuatan atau pendistribusian pesan-pesan yang bersifat mengganggu atau menghina, termasuk di dalamnya pesan-pesan yang menghina ras, gender, warna rambut, cacad tubuh, usia, agama, politik, atau kebangsaan tertentu. Karyawan PT. X yang menerima email seperti itu dari karyawan PT. X lain wajib segera melaporkan hal tersebut kepada atasannya.

**3.2. Penggunaan Pribadi**

Penggunaan sistem email PT. X untuk pengiriman dan/atau penerimaan pesan-pesan pribadi diperbolehkan selama hal tersebut terjadi dalam batas-batas yang wajar. Namun demikian, email yang tidak ada hubungannya dengan pekerjaan wajib disimpan dalam folder terpisah dari email yang berhubungan dengan pekerjaan. Dilarang keras mengirimkan email dari email account PT. X yang bersifat *chain mail* ataupun yang berisi lelucon-lelucon.

**3.3. Pengawasan**

Para karyawan PT. X tidak dapat mengharapkan privasi dalam penggunaan sistem email PT. X. Manajemen PT. X boleh membaca pesan-pesan karyawan baik yang telah disimpan, sedang dikirim, ataupun sedang diterima tanpa pemberitahuan terlebih dahulu. Di lain pihak, manajemen PT. X tidak memiliki kewajiban untuk mengawasi email karyawan.

**4.0. Sanksi**

Karyawan yang terbukti telah melanggar kebijakan ini akan dikenakan sanksi, yang mana bentuk sanksi itu dapat berupa mulai teguran lisan atau tertulis hingga pemutusan hubungan kerja.

**5.0. Definisi**

| **Istilah** | **Definisi** |
|---|---|
| Email | Pengiriman informasi secara elektronik |

| | |
|---|---|
| | menggunakan protocol mail seperti SMTP atau IMAP. Perangkat lunak client untuk email yang biasa dipergunakan adalah Eudora, Mozilla Thunderbird dan Microsoft Outlook. |
| Chain Mail | Email yang dikirimkan ke orang-orang secara berantai. Biasanya pesan yang dikandung memberikan instruksi agar pesan itu diteruskan ke sejumlah orang, dengan janji imbalan nasib mujur atau uang jika instruksi itu dituruti |

**6.0. Sejarah Revisi**

Contoh di atas merupakan contoh sederhana namun efektif dari cara PT. X menyusun kebijakan pengamanan informasi khusus tentang penggunaan sistem email perusahaan. Contoh ini dibuat berdasarkan *template* yang disediakan oleh SANS Institute pada situs web mereka. (SANS, 2006) Pada situs tersebut telah disediakan *templates* untuk kebijakan-kebijakan pengamanan informasi sebagai berikut:

- Acceptable Encryption Policy
- Acceptable Use Policy
- Analog/ISDN Line Policy
- Anti-Virus Process
- Application Service Provider Policy
- Application Service Provider Standards
- Acquisition Assessment Policy
- Audit Vulnerability Scanning Policy
- Automatically Forwarded Email Policy
- Ethics Policy
- Extranet Policy
- Information Sensitivity Policy
- Internal Lab Security Policy
- Internet DMZ Equipment Policy
- Lab Anti-Virus Policy
- Password Protection Policy
- Remote Access Policy
- Risk Assessment Policy
- Router Security Policy
- Server Security Policy

- Database Credentials Coding Policy
- Dial-in Access Policy
- DMZ Lab Security Policy
- E-mail Policy
- 3rd Party Network Connection Agreement
- VPN Security Policy
- Wireless Communication Policy

**5. Peran Kebijakan Pengamanan Informasi dalam Manajemen Risiko Atas Informasi**

Dari pembahasan-pembahasan di atas, maka dapat dilakukan analisa tentang apa saja peran Kebijakan Pengamanan Informasi dalam Manajemen Risiko atas informasi.

Pertama-tama perlu diingat bahwa satu bagian dari manajemen risiko atas informasi adalah penerapan berbagai jenis perangkat pengendali (*controls*) pada sistem informasi perusahaan, dan bahwa *controls* tersebut dapat dibagi menjadi tiga jenis, yaitu: *technical controls, formal controls*, dan *informal controls*.

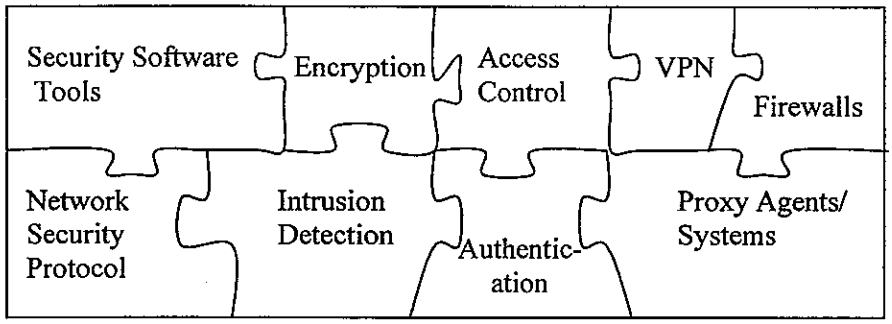
Di atas telah disebutkan bahwa *informal controls* adalah berbagai nilai dan semangat yang ditanamkan manajemen perusahaan ke dalam karyawan perusahaan. Termasuk di sini dapat disebutkan tentang etika bisnis, semangat kebersamaan, dan lain sebagainya. Jika diperhatikan pada daftar *template* kebijakan pengamanan informasi yang disediakan oleh SANS Institute, maka tampak pada kolom kanan terdapat pula sebuah *ethics policy*, yang antara lain menyebutkan bahwa perusahaan menjunjung tinggi praktek-praktek usaha yang berlandaskan etika bisnis yang sehat, bahwa perusahaan mendorong semangat keterbukaan dan kebersamaan pada karyawannya, bahwa eksekutif perusahaan harus terbuka pada segala macam kritik dan saran, dan lain sebagainya. Oleh karena itu, dapat disimpulkan bahwa Kebijakan Pengamanan Informasi dapat berbentuk *informal control*.

Kebijakan Pengamanan Informasi juga dapat berbentuk *formal control*, atau menjadi landasan dalam pembentukan *formal control*. Dalam hal kebijakan tersebut bersifat *issue specific*, seperti misalnya kebijakan tentang penggunaan sistem email perusahaan, atau tentang pembuatan dan penggunaan password, maka kebijakan ini sendiri sudah merupakan *formal control*. Namun kalau kebijakan itu merupakan kebijakan *program-level*, seperti misalnya kebijakan tentang hak dan kewajiban divisi

sistem informasi melakukan *risk assessment* secara berkala, maka kebijakan itu masih harus dijabarkan lebih lanjut agar menjadi *formal control* yang jelas dalam pelaksanaannya.

Dalam hal *technical controls*, seperti instalasi *firewall*, penyiapan perangkat dan sistem enkripsi, dan sebagainya, maka Kebijakan Pengamanan Informasi merupakan acuan yang handal bagi petugas pelaksana. Misalnya saja, untuk masalah monitoring atas email karyawan, apakah petugas pelaksana sebaiknya menyiapkannya atau tidak? Jika dilihat pada contoh kebijakan dari PT. X di atas, maka jelas bahwa petugas pelaksana harus menyiapkan sistem monitoring email untuk digunakan oleh manajemen.

Selain itu, menurut hemat penulis, Kebijakan Pengamanan Informasi ini dapat turut mengarahkan agar supaya semua *technical controls* yang dipasang oleh divisi sistem informasi perusahaan membentuk suatu "pagar" yang rapat dan sulit ditembus oleh pihak-pihak yang mengancam (internal atau eksternal, baik secara sengaja maupun tidak disengaja). James A. O'Brien menggambarkan dalam bukunya bahwa *technical controls* perusahaan sebaiknya dipasang sedemikian rupa sehingga semuanya saling mengunci seperti halnya bagian-bagian dari sebuah *jigsaw puzzle*. (O'Brien, 2004: h. 402)




**Gambar 1. Technical Controls Saling Mengunci**
**(diadaptasi dari O'Brien)**

Berangkat dari kenyataan bahwa sebuah kebijakan dibuat dalam rangka pencapaian tujuan tertentu, maka dalam hal ini tujuan pengamanan sistem informasi perusahaan,

yaitu menjaga *confidentiality, availability*, dan *integrity* informasi, dapat dilihat secara menyeluruh dalam satu *program-level policy*, yang kemudian dijabarkan lebih lanjut dalam sejumlah *issue-specific policies*. Karena kebijakan-kebijakan *issue-specific* itu merupakan turunan dari kebijakan *program-level*, maka otomatis kebijakan-kebijakan itu akan saling mengisi. Apabila kemudian *technical controls* diterapkan sebagai realisasi dari kebijakan-kebijakan *issue-specific* tadi, maka diharapkan secara langsung terjadi dorongan dan tekanan pada pihak yang memasang *technical controls* tersebut agar memenuhi kriteria "*interlocking*" tersebut.

**6. Kesimpulan**

Dari pembahasan di atas, akhirnya dapat disimpulkan bahwa peran Kebijakan Pengamanan Informasi dalam usaha manajemen risiko atas informasi adalah:

- Kebijakan Pengamanan Informasi dapat berperan sebagai *informal control.*
- Kebijakan Pengamanan Informasi yang bersifat *issue-specific* berperan sebagai *formal control.*
- Kebijakan Pengamanan Informasi yang bersifat *program-level* berperan sebagai rujukan untuk peraturan-peraturan yang menjadi *formal control.*
- Kebijakan Pengamanan Informasi berperan sebagai koordinator agar semua usaha *technical control* dibuat dan dilaksanakan sedemikian rupa sehingga saling mengunci rapat, sehingga tidak ada pihak yang mengancam (*threats*) yang dapat menembusnya.

Oleh karena itu, dapat disimpulkan lebih lanjut bahwa Kebijakan Pengamanan Informasi (*Information Security Policy*) memiliki peran yang sentral pada semua level manajemen risiko atas informasi. Tentu perlu ditambahkan di sini bahwa setiap kebijakan tanpa pelaksanaan dan pengawasan yang baik tidak akan berguna. Jadi meskipun kebijakan seperti ini jelas sangat penting, namun tidaklah cukup untuk meyakinkan terlaksananya manajemen risiko dengan baik dan benar.

## 7. Daftar Pustaka

[1] Anonim, *Manajemen Risiko: Peranan dan Proses Manajemen Risiko*, Mod.02, Handout Pelatihan Telkom.

[2] Dale Walter Karolak (1996), *Software Engineering Risk Management*, IEEE Computer Society Press, Los Alamitos.

[3] Raymond McLeod, Jr. and George P. Schell (2004), *Management Information Systems*, 9th edition, Pearson/Prentice-Hall, New Jersey.

[4] Micki Krause, and Harold F. Tipton, *Handbook of Information Security Management*, CRC Press LCC, http://www.ccert.edu.cn/education/cissp/hism/ewtoc.html, diakses tanggal 9 April 2006 jam 17:31.

[5] Ed Roback (ed.) (Oct. 16, 2002), *Computer and Information Security Policy: Draft Paper for NIST Computer Security Handbook.* http://www.windowsecurity.com/pages/article_p.asp?id=871 diakses tanggal 9 April 2006 jam 20:01.

[6] The SANS Security Policy Project, http://www.sans.org/resources/policies/, diakses tanggal 9 April 2006 jam 19:04.

[7] James A. O'Brien (2004), *Management Information Systems*, 6th edition, McGraw-Hill, Boston.