# RISK ASSESSMENT

**Yusup Jauhari Shandi**

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. H. Juanda Bandung 40132

**ABSTRAK**

Sebuah sistem informasi merupakan aset yang bisa disejajarkan dengan gedung, kendaraan dan lainnya dalam sebuah organisasi. Maka dari itu kebutuhan keamanan akan sistem menjadi hal yang harus diperhatikan juga oleh organisasi. Sumber ancaman terhadap sistem diantaranya: ancaman dari alam, manusia serta lingkungan. Dengan melakukan tahapan-tahapan penilaian resiko diharapkan proses pengambilan keputusan terhadap aksi yang akan dilakukan berkaitan dengan ancaman terhadap sistem menjadi lebih jelas serta memudahkan dalam menentukan prioritas terhadap aksi yang akan dilakukan.

**Kata-kata kunci:** ancaman, resiko

## 1. PENDAHULUAN

Setiap organisasi memiliki proses bisnis untuk menjalankan kegiatan usahanya. Sistem Informasi adalah salah satu alat pembantu untuk menjalankan proses bisnis tersebut. Kebutuhan-kebutuhan akan informasi diharapkan bisa terpenuhi dengan adanya sistem informasi. Implementasi proses bisnis melalui sistem informasi ini diterapkan mulai dari proses yang sifatnya transaksional sampai pendukung keputusan bagi managemen tingkat atas. Pengembangan sebuah sistem informasi bagi organisasi membutuhkan biaya. Besarnya biaya tergantung dari kompleksitas dari proses bisnis organisasi tersebut. Oleh karena itu sistem informasi bisa juga disebut sebagai *asset* organisasi.

Sebuah *asset* haruslah dipelihara dan dijaga agar tetap memberikan manfaat bagi organisasi tersebut. Organisasi yang baik haruslah menyediakan anggaran untuk perawatan serta pengembangan untuk sistem yang dimilikinya. Pada proses implementasi sistem biasanya akan ditemukan masalah-masalah yang bisa menimbulkan gangguan terhadap sistem. Masalah tersebut bisa berasal dari sistem itu sendiri atau dari luar sistem. Akibat dari masalah tersebut adalah munculnya resiko-resiko terhadap sistem.

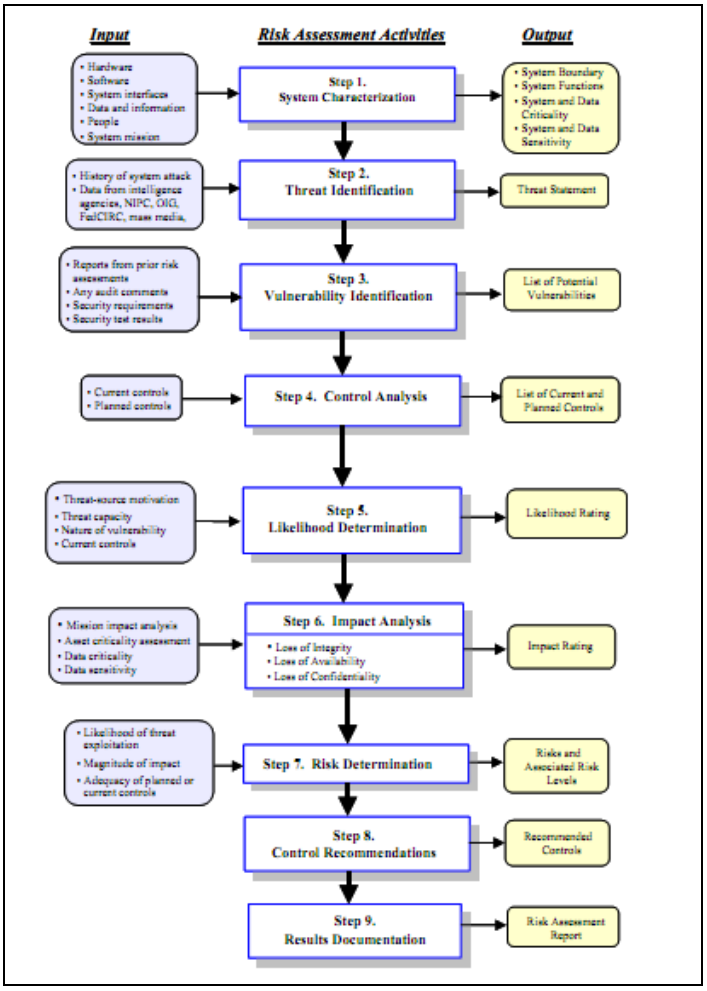
Penilaian resiko terhadap semua komponen sistem informasi yang dimiliki oleh organisasi diharapkan dapat memberikan masukan untuk mendukukung keputusan manajemen dalam hal pengelolaan resiko dalam sistem yang dimilikinya.

## 2. RISK ASSESSMENT

*Risk assessment* adalah proses pertama dari *risk management methodology*[2]. *Risk assessment* digunakan oleh organisasi untuk menentukan lebih jauh sebuah potensi ancaman dan resiko yang berhubungan dengan sistem IT. Hasil dari proses *risk assessment* bisa dimanfaatkan untuk mengidentifikasi penanganan yang harus dilakukan untuk mengurangi atau menghilangkan resiko pada tahapan *risk management methodology* selanjutnya yaitu *risk mitigation*[1].

Resiko di sini memiliki pengertian sebagai sesuatu kemungkinan yang ditimbulkan oleh sumber-sumber ancaman terhadap kerentanan yang ada pada sistem yang bisa mengakibatkan kerugian bagi organisasi.

Untuk bisa menentukan kemungkinan gangguan yang bisa mengakibatkan kerugian nantinya, ancaman terhadap sistem harus bisa dianalisa hubungan atau keterkaitannya terhadap sumber-sumber kerentanan yang ada pada sistem serta kontrol apa yang harus dilakukan.




*Risk assessment steps* [1]

Ada 9 langkah untuk melakukan *risk assessment* yaitu :

1. ***System Characterization***

   Pada tahap ini dilakukan proses-proses seperti definisi ruang lingkup sistem serta mengidentifikasi batasan sistem. Pada proses ini diharapkan menghasilkan gambaran mengenai ruang lingkup penilaian resiko, deskripsi mengenai otorisasi operasional sistem, serta tersedianya informasi yang diperlukan untuk mendefinisikan resiko (mengenai *hardware*, *software*, jaringan, bagian atau pihak yang bertanggung jawab terhadap sistem).

2. ***Threat Identification***

   Pada tahap ini dilakukan proses identifikasi ancaman-ancaman yang berpotensi menyerang kerentanan sistem. Sebuah ancaman tidak akan mendatangkan resiko

jika tidak ada kerentanan dari sistem yang bisa diserang. Proses *threat identification* dibagi menjadi dua kegiatan, yaitu:

a. *Threat-source identification*, yaitu proses mengidentifikasi sumber-sumber ancaman.
b. *Motivation and Threat action*, yaitu proses mengidentifikasi motivasi dari ancaman-ancaman yang mungkin terjadi. Perlu diketahui bahwa motivasi hanya dimiliki oleh sumber ancaman yang berasal dari manusia. Sebagai contoh bisa dilihat pada tabel di bawah berikut:

| **Sumber ancaman** | **Motivasi** | **Aksi** |
|---|---|---|
| Hacker, cracker | Tantangan, pemberontakan, ego, penghianatan, uang | *Hacking*, *social engineering*, *carding*, *defacing*, dan sebagainya |
| Mata-mata perusahaan | Keuntungan persaingan usaha | Pencurian informasi, pembobolan sistem |
| Bencana alam | - | Merusak *server*, infrastruktur |
| | | |

***3. Vulnerability Identification***

Pada tahap ini dilakukan proses identifikasi kerentanan atau kelemahan yang ada pada sistem yang bisa dimanfaatkan oleh sumber-sumber ancaman yang tadi telah didefinisikan pada tahap sebelumnya. Berikut contoh hasil dari tahap ini :

| **Kerentantan sistem** | **Sumber ancaman** | **Aksi sumber ancaman** |
|---|---|---|
| Tidak terhapusnya ID dari pegawai yang sudah tidak aktif | Dari pegawai yang bersangkutan | Merubah atau mencuri data |
| Penggunaan alarm kebakaran dengan siraman air di ruang server | Kebakaran, orang jahil | Perangkat keras rusak tersiram air |

***4. Control Analysis***

Pada tahap ini dilakukan proses analisa terhadap kontrol-kontrol pengamanan yang telah atau akan diterapkan oleh organisasi dalam rangka mengurangi atau

menghilangkan kemungkinan gangguan oleh sumber ancaman terhadap kerentanan sistem.

***5. Likelihood Determination***

Pada tahap ini ditentukan tingkatan-tingkatan nilai atau level dari kemungkinan ancaman-ancaman yang sudah didefinisikan. Tingkatan-tingkatan tersebut misal dibuat seperti berikut:

| **Level** | **Definisi** |
|---|---|
| Tinggi | Sumber ancaman sangat mungkin terjadi dan termotivasi dan kontrol untuk menanganinya sangat tidak efektif atau belum ada |
| Sedang | Sumber ancaman mungkin terjadi dan termotivasi dan kontrol untuk menanganinya sudah ada |
| Rendah | Sumber ancaman hampir tidak ada atau tidak terjadi dan tidak termotivasi dan kontrol untuk menanganinya sudah ada |

***6. Impact Analisys***

Pada tahap ini ditentukan dampak yang merugikan terhadap sistem jika sumber ancaman berhasil memanfaatkan kerentanan yang ada pada sistem. Besarnya dampak dari sumber ancaman bisa digambarkan sebagai berikut:

| **Dampak** | **Definisi dampak** |
|---|---|
| Tinggi | Aksi dari sumber ancaman terhadap kerentanan sistem telah terjadi sehingga mengakibatkan kerugian yang sangat besar pada organisasi berupa: biaya yang tinggi untuk memperbaiki kerusakan sistem, nama buruk organisasi, kecelakaan bahkan kematian pegawai. |
| Sedang | Aksi dari sumber ancaman terhadap kerentanan sistem telah terjadi sehingga mengakibatkan kerugian tidak terlalu besar pada organisasi berupa: biaya untuk memperbaiki kerusakan sistem, nama buruk organisasi, kecelakaan pegawai. |
| Rendah | Aksi dari sumber ancaman terhadap kerentanan sistem telah terjadi sehingga mengakibatkan sedikit kerugian pada organisasi berupa: kemungkinan dikeluarkan biaya untuk perbaikan sistem, ganguan transaksional yang mengakibatkan tertundanya proses dalam waktu relatif singkat. |

### *7. Risk Determination*

Pada tahap ini ditentukan penilaian terhadap level resiko yang bisa terjadi pada sistem. Pada tahap ini dibuat matriks untuk menentukan nilai resiko, misal seperti berikut:

| Threat Likelihood | Impact | | |
|---|---|---|---|
| | ***Low*** (10) | ***Medium*** (50) | ***High*** (100) |
| ***High*** (1.0) | **Low** 10 X 1.0 = 10 | **Medium** 50 X 1.0 = 50 | **High** 100 X 1.0 = 100 |
| ***Medium*** (0.5) | **Low** 10 X 0.5 = 5 | **Medium** 50 X 0.5 = 25 | **Medium** 100 X 0.5 = 50 |
| ***Low*** (0.1) | **Low** 10 X 0.1 = 1 | **Low** 50 X 0.1 = 5 | **Low** 100 X 0.1 = 10 |

*Risk Scale: High ( >50 to 100); Medium ( >10 to 50); Low (1 to 10)*[8]

Penjelasan mengenai matriks tersebut adalah :

| **Level Resiko** | **Deskripsi resiko dan penanggulannya** |
|---|---|
| Tinggi | Kebutuhan perbaikan sangat dibutuhkan untuk dilakukan. Sistem tetap berjalan, tetapi perbaikan harus segera dilakukan secepatnya. |
| Sedang | Perbaikan sistem dibutuhkan dan harus segera dibuat perencanaan dari proses perbaikan sistem. |
| Rendah | Perbaikan sistem bisa dilakukan atau resiko bisa diterima. |

### *8. Control Recomendation*

Pada tahap ini dilakukan pembuatan rekomendasi kontrol yang harus dilakukan berdasarkan data-data pada tahap-tahap selanjutnya. Rekomendasi ini digunakan untuk mengurangi level resiko terhadap sistem pada titik level aman. Beberapa faktor yang harus diperhatikan pada tahap ini adalah :

a. Rekomendasi yang efektif
b. Legislasi dan regulasi
c. Kebijakan organisasi
d. Dampak operasional
e. Keamanan dan tahan uji

Perlu diketahui bahwa tidak semua kontrol yang diusulkan bisa mengurangi kerugian.

***9. Results Documentation***

Pada tahap terakhir ini dibuat dokumentasi sebagai rangkuman dari seluruh tahap *risk assessment*. Dimana dengan dokumentasi atau laporan ini pihak-pihak yang berkepentingan bisa dibantu dalam rangka menentukan kebijakan, prosedur, biaya terhadap perbaikan sistem.

## 3. KESIMPULAN

*Risk assessment* adalah salah satu tahapan dari *risk management methodology*. *Risk assessment* digunakan oleh organisasi untuk menentukan lebih jauh sebuah potensi ancaman dan resiko yang berhubungan dengan sistem IT. Tahapan-tahapan *risk assessment* harus dilakukan agar diperoleh hasil akhir berupa laporan hasil penilaian resiko-resiko yang ada dan bisa mengakibatkan dampak negatif pada sistem organisasi tersebut. Dengan laporan ini maka pihak organisasi bisa lebih mudah menentukan aksi yang harus dilakukan dalam segala aspek untuk keamansan sistem yang dimilikinya. Selain itu laporan ini berguna sebagai masukan untuk tahapan *risk management methodology* lainnya yaitu *risk mitigation*.

## 4. DAFTAR PUSTAKA

1. Gary Stoneburner, Alice Goguen, Alexis Feringa, *Risk Management Guide for Information Technology Systems*, July 2002, NIST Special Publication 800-30.

2. Marianne Swanson, Barbara Guttman, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996, National Institute of Standards and Technology NIST.