Strategi Pendekatan Manajemen Resiko Dalam Pengembangan Sistem Informasi

1. PENDAHULUAN

Resiko adalah suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisa serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko.

1. PENDAHULUAN

Pada dasarnya, faktor resiko dalam suatu perencanaan sistem informasi, dapat diklasifikasikan ke dalam 4 kategori resiko, yaitu :

a. *Catastrophic* (Bencana)
b. *Critical* (Kritis)
c. *Marginal* (kecil)
d. *Negligible* (dapat diabaikan)

1. PENDAHULUAN

Adapun pengaruh atau dampak yang ditimbulkan terhadap suatu proyek sistem informasi dapat berpengaruh kepada

a. Nilai unjuk kerja dari sistem yang dikembangkan,
b. Biaya yang dikeluarkan oleh suatu organisasi yang mengembangkan teknologi informasi,
c. Dukungan pihak manajemen terhadap pengembangan teknologi informasi, dan
d. Skedul waktu penerapan pengembangan teknologi informasi.

1. PENDAHULUAN

- Suatu resiko perlu didefinisikan dalam suatu pendekatan yang sistematis, sehingga pengaruh dari resiko yang timbul atas pengembangan teknologi informasi pada suatu organisasi dapat diantisipasi dan di identifikasi sebelumnya

2. POLA PENDEKATAN

- *System Development Life Cycle* [SDLC] adalah suatu tahapan proses perancangan suatu sistem yang dimulai dari tahap investigasi; pembangunan; implementasi; operasi/perawatan; serta tahap penyelesaian.
- Dari dasar tersebut di atas, strategi penerapan manajemen resiko perlu mempertimbangkan dampak yang mungkin timbul dengan tingkat probabilitas yang berbeda untuk setiap komponen pengembangan sistem informasi.

2. POLA PENDEKATAN

- Pola pendekatan manajemen resiko juga perlu mempertimbangkan faktor-faktor pada *System Development Life Cycle* (SDLC) yang terintegrasi, yaitu Mengindentifikasikan faktor-faktor resiko yang timbul dan diuraikan disetiap tahap perancangan sistem, yang tersusun sebagai berikut :

2. POLA PENDEKATAN

- ***Tahap 1. Investigasi (Inisiasi)***

  Tahap ini suatu sistem didefinisikan, menyangkut ruang lingkup pengembangan yang akan dibuat, yang semua perencanaan atas pengembangan sistem di dokumentasikan terlebih dahulu. Dukungan yang dibutuhkan dari manajemen resiko pada tahap ini adalah faktor resiko yang mungkin terjadi dari suatu sistem informasi di identifikasikan, termasuk di dalamnya masalah serta konsep pengoperasian keamanan sistem yang semuanya bersifat strategis.

2. POLA PENDEKATAN

- ***Tahap 2. Pengembangan (planning)***

  Tahap ini merupakan tahap dimana suatu sistem informasi dirancang, pembelian komponen pendukung sistem di laksanakan, aplikasi di susun dalam program tertentu, atau masa dimana konstruksi atas sistem di laksanakan. Pada proses ini, faktor resiko diidentifikasikan selama tahap ini dilalui, dapat berupa analisa atas keamanan sistem sampai dengan kemungkinan yang timbul selama masa konstruksi sistem di laksanakan.

2. POLA PENDEKATAN

- ***Tahap 3. Implementasi (development, controlling, closing)***

  Tahap ini kebutuhan atas keamanan sistem dikonfigurasikan, aplikasi sistem di uji coba sampai pada verifikasi atas suatu sistem informasi di lakukan. Pada tahap ini faktor resiko di rancang guna mendukung proses pelaksanaan atas implementasi sistem informasi sehingga kebutuhan riil di lapangan serta pengoperasian yang benar dapat dilaksanakan.

2. POLA PENDEKATAN

- ***Tahap 4. Pengoperasian dan Perawatan***

  Tahap ini merupakan tahap dimana sistem informasi telah berjalan sebagaimana mestinya, akan tetapi secara berkala sistem membutuhkan modifikasi, penambahan peralatan baik perangkat keras maupun perangkat lunak pendukung, perubahan tenaga pendukung operasi, perbaikan kebijakan maupun prosedur dari suatu organisasi. Pada tahap ini manajemen resiko lebih menitik beratkan pada kontrol berkala dari semua faktor yang menentukan berjalannya sistem, seperti perangkat keras, perangkat lunak, analisa sumber daya manusia, analisa basis data, maupun analisa atas jaringan sistem informasi yang ada.

2. POLA PENDEKATAN

- **Tahap 5. Penyelesaian/penyebaran**

  Tahap ini merupakan tahap dimana system informasi yang telah digunakan perlu di lakukan investasi baru karena performansi atas sistem tersebut telah berkurang, sehingga proses pemusnahan data, penggantian perangkat keras dan perangkat lunak, ataupun berhentinya kegiatan atau kepindahan organisasi ke tempat yang baru. Manajemen resiko yang perlu di perhatikan dalam tahap ini adalah memastikan proses pemusnahan atas komponen-komponen system informasi dapat berjalan dengan baik, terkelola dari segi keamanan.

  Setelah pola pendekatan manajemen resiko di definisikan dalam masing-masing tahap SDLC, maka tahap selanjutnya adalah menilai manajemen resiko dalam metodologi tertentu. Upaya memberikan penilaian atas dampak resiko dalam pengembangan sistem informasi, perlu dilakukan karena dapat memberikan gambaran atas besar atau kecilnya dampak ancaman yang mungkin timbul selama proses pengembangan sistem.

3. METODOLOGI PENILAIAN RESIKO

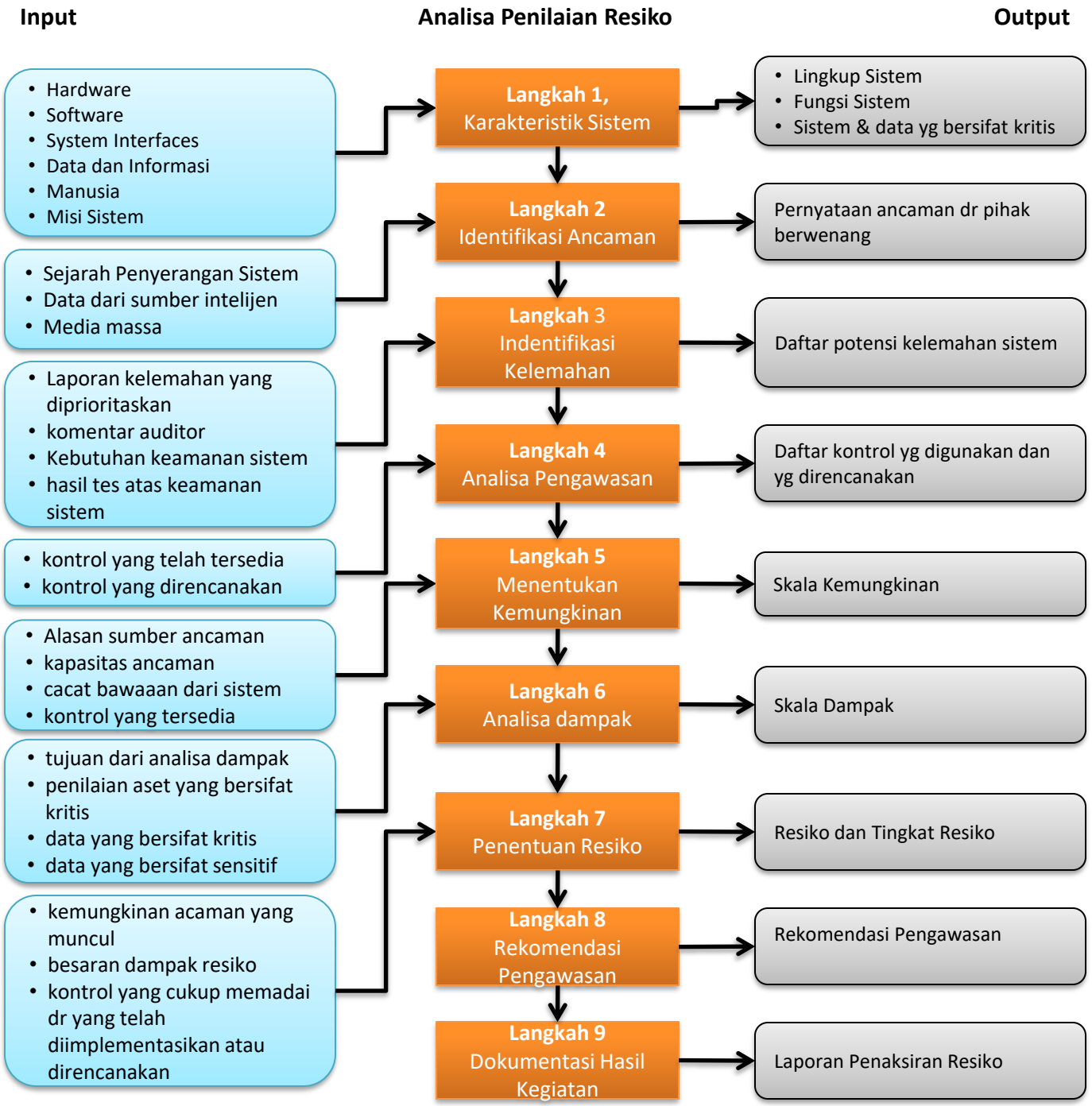
- Untuk menentukan kemungkinan resiko yang timbul selama proses pengembangan sistem informasi berlangsung, maka organisasi yang bermaksud mengembangkan sistem informasi perlu menganalisa beberapa kemungkinan yang timbul dari pengembangan sistem informasi tersebut. Adapun metodologi penilaian resiko pengembangan sistem informasi dapat diuraikan dalam 9 langkah, yang tersusun sebagai berikut :

3. METODOLOGI PENILAIAN RESIKO

a. Menentukan karakteristik dari suatu sistem
b. Mengidentifikasikan ancaman-ancaman
c. Mengidentifikasikan kelemahan sistem
d. Menganalisa pengawasan
e. Menentukan beberapa kemungkinan pemecahan masalah
f. Menganalisa pengaruh resiko terhadap pengembangan sistem
g. Menentukan resiko
h. Merekomendasikan cara-cara pengendalian resiko
i. Mendokumentasikan hasil keputusan

3. METODOLOGI PENILAIAN RESIKO

- Tahap ke dua, tiga, empat dan enam dari langkah tersebut di atas dapat dilakukan secara paralel setelah langkah pertama dilaksanakan. Adapun gambaran dari setiap langkah tersebut adalah sebagai berikut :


Input
Analisa Penilaian Resiko
Output
• Hardware
• Software
• System Interfaces
• Data dan Informasi
• Manusia
• Misi Sistem
Langkah 1, Karakteristik Sistem
• Lingkup Sistem
• Fungsi Sistem
• Sistem & data yg bersifat kritis
• Sejarah Penyerangan Sistem
• Data dari sumber intelijen
• Media massa
Langkah 2 Identifikasi Ancaman
Pernyataan ancaman dr pihak berwenang
• Laporan kelemahan yang diprioritaskan
• komentar auditor
• Kebutuhan keamanan sistem
• hasil tes atas keamanan sistem
Langkah 3 Indentifikasi Kelemahan
Daftar potensi kelemahan sistem
• kontrol yang telah tersedia
• kontrol yang direncanakan
Langkah 4 Analisa Pengawasan
Daftar kontrol yg digunakan dan yg direncanakan
• Alasan sumber ancaman
• kapasitas ancaman
• cacat bawaaan dari sistem
• kontrol yang tersedia
Langkah 5 Menentukan Kemungkinan
Skala Kemungkinan
• tujuan dari analisa dampak
• penilaian aset yang bersifat kritis
• data yang bersifat kritis
• data yang bersifat sensitif
Langkah 6 Analisa dampak
Skala Dampak
• kemungkinan acaman yang muncul
• besaran dampak resiko
• kontrol yang cukup memadai dr yang telah diimplementasikan atau direncanakan
Langkah 7 Penentuan Resiko
Resiko dan Tingkat Resiko
Langkah 8 Rekomendasi Pengawasan
Rekomendasi Pengawasan
Langkah 9 Dokumentasi Hasil Kegiatan
Laporan Penaksiran Resiko

3. METODOLOGI PENILAIAN RESIKO

- ***Langkah 1. Menentukan Karakterisasi Sistem***

  Pada langkah pertama ini batasan suatu sistem yang akan dikembangan di identifikasikan, meliputi perangkat keras, perangkat lunak, sistem interface, data dan informasi, sumber daya manusia yang mendukung sistem IT, tujuan dari sistem, sistem dan data kritis, serta sistem dan data sensitif. Beberapa hal tambahan yang dapat diklasifikasikan pada karakteristik sistem selain hal tersebut di atas seperti bentuk dari arsitektur keamanan sistem, kebijakan yang dibuat dalam penanganan keamanan sistem informasi, bentuk topologi jaringan komputer yang dimiliki oleh organisasi tersebut, Manajemen pengawasan yang dipakai pada sistem TI di organisasi tersebut, dan hal lain yang berhubungan dengan masalah keamanan seputar penerapan Teknologi Informasi di organisasi yang bermaksud mengembangkan sistem informasi.

3. METODOLOGI PENILAIAN RESIKO

Langkah 1. Menentukan Karakterisasi Sistem – cont'd

Adapun teknik pengumpulan informasi yang dapat diterapkan pada langkah ini meliputi :

1. ***Membuat daftar kuesinoner***. Daftar kuesioner ini di susun untuk semua level manajemen yang terlibat dalam sistem dengan tujuan mengumpulkan informasi seputar keamanan data dan informasi dengan tujuan untuk memperoleh pola resiko yang mungkin dihadapi oleh sistem.
2. ***Interview*****.** Bentuk lain dari pengumpulan data dengan cara interview terhadap IT Support atau personil yang terlibat dalam sistem informasi.
3. ***Review atas dokumen*****.** Review atas dokumen pengembangan sistem, Dokumen kebijakan, atau dokumen keamanan informasi dapat memberikan gambaran yang bermanfaat tentang bentuk dari kontrol yang saat ini diterapkan oleh SI maupun rencanan pengembangan dari pengawasan di masa depan.
4. ***Penerapan Tool*****.** Menggunakan suatu tool aplikasi yang memiliki tujuan untuk mengumpulkan informasi tentang sistem informasi yang digunakan merupakan salah satu cara untuk dapat memetakan sistem secara keseluruhan, seperti penggunakan network monitor, maupun tools lain.

3. METODOLOGI PENILAIAN RESIKO

Langkah 1. Menentukan Karakterisasi Sistem – cont'd

Hasil output dari langkah pertama ini akan menghasilkan Penaksiran atas karakteristik sistem IT, Gambaran tentang lingkungan sistem IT serta gambaran tentang batasan dari sistem yang dikembangkan.

3. METODOLOGI PENILAIAN RESIKO

- ***Langkah 2. Mengidentifikasikan ancaman-ancaman***

  Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Timbulnya ancaman dapat dipicu oleh suatu kondisi dari sumber ancaman. Sumber ancaman dapat muncul dari kegiatan pengolahan informasi yang berasal dari 3 hal utama, yaitu

  1. Ancaman Alam;
  2. Ancaman Manusia, dan
  3. Ancaman Lingkungan.

  Ancaman yang berasal dari manusia memiliki karakteristik tersendiri, serta memiliki alasan tersendiri dalam melakukan gangguan terhadap sistem informasi yang ada. Adapun alasan yang timbul dari ancaman manusia ini dapat di definisikan dalam tabel berikut :

Langkah 2. Mengidentifikasikan ancaman-ancaman dari manusia

Sumber ancaman	Alasan	Aksi yang timbul
Hacker, Cracker	• Tantangan • Ego • Memberontak	• Hacking • Social Engineering • Gangguan sistem • Akses terhadap sistem
Kriminal	• Perusakan informasi • Penyingkapan informasi secara ilegal • Keuntungan moneter • Merubah data	• Tindak Kriminal • Perbuatan curang • Penyuapan • Spoofing • Intrusi atas sistem
Teroris	• Surat kaleng • Perusakan • Peledakan • Balas dendam	• Bom/teror • Perang informasi • Penyerangan sistem • Penembusan atas sistem • Tampering sistem
Mata-mata	• Persaingan usaha • Mata-mata ekonomi	• Pencurian informasi • Social engineering • Penembusan atas sistem
Orang dalam Organisasi	• Keingintahuan • Ego • Mata-mata • Balas dendam • Kelalaian kerja	• Surat kaleng • Sabotase atas sistem • Bug sistem • Pencurian/penipuan • Perubahan data • Virus, trojan, dll • Penyalahgunaan komputer

3. METODOLOGI PENILAIAN RESIKO

Langkah 2. Mengidentifikasikan ancaman-ancaman - cont'd

Organisasi yang membutuhkan daftar dari sumber ancaman, perlu melakukan hubungan dengan badan-badan atau sumber-sumber yang berhubungan dengan keamanan, seperti misalnya sumber ancaman dari alam diharapkan hubungan dengan BMG yang menangani masalah alam, atau pihak intelijen atau media massa yang dapat mendeteksi sumber ancaman dari manusia. Hasil output dari ancaman ini merupakan pernyataan atau daftar yang berisikan sumber ancaman yang mungkin dapat mengganggu sistem secara keseluruhan.

3. METODOLOGI PENILAIAN RESIKO

Langkah 3. Identifikasi kelemahan

- Cacat atau kelemahan dari suatu sistem adalah suatu kesalahan yang tidak terdeteksi yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh sumber ancaman yang mencoba menyusup terhadap sistem tersebut.
- Pada beberapa vendor besar, informasi atas kelemahan sistem yang dibuat oleh vendor tersebut ditutup atau dihilangkan dengan penyediaan layanan purna jual dengan menyediakan hot fixes, service pack, pathces ataupun bentuk layanan lain.

3. METODOLOGI PENILAIAN RESIKO

Langkah 3. Identifikasi kelemahan **- cont'd**

Penerapan metode proaktif atau tersedianya karyawan yang bertugas untuk melakukan sistem test dapat di pakai untuk mencek kelemahan sistem secara efisien, dimana hal tersebut tergantung kepada keberadaan sumber daya atau kondisi IT yang bersifat kritis. Metode tes yang diterapkan dapat berbentuk :

- Penggunaan tool yang menscan kelemahan sistem secara automatis
- Adanya Evaluasi dan sekuriti tes (ST&E), atau
- Melakukan penetrasi tes

3. METODOLOGI PENILAIAN RESIKO

Langkah 3. Identifikasi kelemahan **- cont'd**

Bentuk keluaran yang timbul pada langkah ketiga ini memungkinkan pihak penilai resiko mendapatkan daftar dari kelemahan sistem yang dapat dianggap sebagai potensi dari sumber ancaman di kemudian hari.

3. METODOLOGI PENILAIAN RESIKO

Langkah 4. Analisa pengawasan

Tujuan yang diharapkan pada langkah ini adalah untuk menganalisa penerapan kontrol yang telah diimplementasikan atau yang direncanakan. Bagi organisasi langkah ini perlu untuk meminimalisasi atau bahkan mengeliminasi probabilitas kemungkinan yang timbul dari sumber ancaman atau potensi kelemahan atas sistem.

3. METODOLOGI PENILAIAN RESIKO

Langkah 4. Analisa pengawasan – Cont'd

Metode pengawasan

Metode pengawasan terdiri atas metode yang bersifat teknis maupun non teknis. Metode pengawasan secara teknis merupakan salah satu upaya perlindungan kepada organisasi dalam hal perlindungan terhadap perangkat keras komputer, perangkat lunak maupun mekanisme akses kontrol yang digunakan, sedangkan metode nonteknis lebih ditekankan kepada pengawasan atas manajemen dan operasional penggunaan sistem IT di organisasi tersebut, seperti penerapan policy keamanan, prosedur operasional, maupun manajemen personel yang ada.

3. METODOLOGI PENILAIAN RESIKO

Langkah 4. Analisa pengawasan – Cont'd

Kategori pengawasan

Kategori pengawasan baik secara teknis maupun non teknis dapat diklasifikasikan dalam 2 pendekatan yaitu pendekatan preventif atau detektif.

3. METODOLOGI PENILAIAN RESIKO

Langkah 4. Analisa pengawasan – Cont'd

- **Pendekatan preventif** adalah upaya untuk mencegah upaya pelanggaran atas policy keamanan seperti pengaksesan atas sistem IT atau tindakan lain misalnya dengan cara mengenkripsi informasi atau menerapkan otentifikasi atas informasi.
- **Pendekatan detektif** adalah cara untuk memperingati pengguna atas terjadinya pelanggaran atau percobaan pelanggaran atas policy keamanan yang ada, metode ini contoh pada Microsoft Windows dengan menggunakan teknik audit trails, metode deteksi penyusupan atau teknik checksum.

3. METODOLOGI PENILAIAN RESIKO

Langkah 4. Analisa pengawasan – cont'd

Teknis analisa pengawasan

- Analisa pengawasan atas policy keamanan dapat menggunakan teknik checklist pengguna yang mengakses sistem IT atau dengan penggunaan checklist yang tersedia untuk memvalidasi keamanan, hal paling penting pada tahap ini adalah mengupdate terus menerus atas checklist pengguna sistem untuk mengontrol pemakai.
- Hasil yang diharapkan muncul pada tahap ini adalah tersedianya daftar kontrol yang digunakan dan yang sedang direncanakan oleh sistem IT untuk memitigasi kemungkinan adanya kelemahan atas sistem dan memperkecil dampak yang mungkin timbul atas penerapan policy keamanan.

3. METODOLOGI PENILAIAN RESIKO

Langkah 5. Menerapkan beberapa kemungkinan

Pada langkah ini, semua skalabilitas kemungkinan yang mungkin timbul dari kelemahan sistem didefinisikan. Terdapat beberapa faktor yang perlu dipertimbangkan dalam upaya mendefinisikan skalabilitas seperti :

- Motif dan kapabilitas dari sumber ancaman
- Kelemahan bawaan dari sistem
- Eksistensi dan efektifitas kontrol yang di terapkan

3. METODOLOGI PENILAIAN RESIKO

Langkah 5. Menerapkan beberapa kemungkinan

Adapun level skalabilitas dari ancaman menurut Roger S. Pressman, dapat di definisikan dalam 4 kategori yang didefinisi dalam tabel berikut :

3. METODOLOGI PENILAIAN RESIKO

Langkah 5. Menerapkan beberapa kemungkinan – Cont'd

Tingkat Ancaman	Definisi
Catastrophics	Pada level ini tingkat ancaman dapat dikategorikan sangat merusak, dimana sumber ancaman memiliki motif besar saat melakukan kegiatannya. dampak yang ditimbulkan dari tingkat ini dapat membuat sistem tidak berfungsi sama sekali.
Critical	Level ini dapat dikategorikan cukup membuat merusak sistem IT, akan tetapi penggunaan kontrol yang diterapkan pada sistem telah dapat menahan kondisi kerusakan sehingga tidak menyebabkan kerusakan yang besar pada sistem.
Marginal	Pada level ini kontrol keamanan mampu mendeteksi sumber ancaman yang menyerang sistem IT, walau tingkat kerusakan pada sistem masih terjadi akan tetapi masih dapat di perbaiki dan dikembalikan kepada kondisi semula
Negligible	Pada level ini sumber ancaman tidak dapat mempengaruhi sistem, dimana kontrol atas sistem sangat mampu mengantisipasi adanya kemungkinan ancaman yang dapat mengganggu sistem

3. METODOLOGI PENILAIAN RESIKO

Langkah 5. Menerapkan beberapa kemungkinan – Cont'd

Hasil dari langkah kelima ini adalah terdefinisikan ancaman dalam beberapa tingkat tertentu, yaitu *kategori catastrophic, critical, marginal* atau negligible

3. METODOLOGI PENILAIAN RESIKO

Langkah 6. Analisa dampak

Analisa dampak merupakan langkah untuk menentukan besaran dari resiko yang memberi dampak terhadap sistem secara keseluruhan. Penilaian atas dampak yang terjadi pada sistem berbeda-beda dimana nilai dari dampak sangat tergantung kepada

- Tujuan sistem IT tersebut saat di kembangkan
- Kondisi sistem dan data yang bersifat kritis, apakah dikategorikan penting atau tidak
- Sistem dan data yang bersifat sensitif

3. METODOLOGI PENILAIAN RESIKO

Langkah 6. Analisa dampak – Cont'd

Dampak yang ditimbulkan oleh suatu ancaman maupun kelemahan, dapat dianalisa dengan mewawancarai pihak-pihak yang berkompeten, sehingga didapatkan gambaran kerugian yang mungkin timbul dari kelemahan dan ancaman yang muncul. Adapun dampak kerugian yang mungkin timbul dari suatu resiko dikategorikan dalam 3 (tiga) kemungkinan yang mana dampak tersebut dapat berkonsekuensi atas satu atas kombinasi dari ketiga hal tersebut. Dampak yang timbul dapat mengarah kepada :

3. METODOLOGI PENILAIAN RESIKO

Langkah 6. Analisa dampak – Cont'd

- ***Dampak atas Confidentiality (Kenyamanan).***

  Dampak ini akan berakibat kepada sistem dan kerahasiaan data dimana sumber daya indormasi akan terbuka dan dapat membahayakan keamanan data. Penyingkapan atas kerahasiaan data dapat menghasilkan tingkat kerugian pada menurunnya kepercayaan atas sumber daya informasi dari sisi kualitatif, sedang dari sisi kuantitatif adalah munculnya biaya perbaikan sistem dan waktu yang dibutuhkan untuk melakukan recovery atas data

3. METODOLOGI PENILAIAN RESIKO

Langkah 6. Analisa dampak – Cont'd

- ***Dampak atas Integrity (Integritas)***

  Dampak integritas adalah termodifikasikan suatu informasi, dampak kualitatif dari kerugian integrity ini adalah menurunkan tingkat produktifitas kerja karena gangguan atas informasi adapun dampak kuantitatif adalah kebutuhan dana dan waktu merecovery informasi yang berubah.

3. METODOLOGI PENILAIAN RESIKO

Langkah 6. Analisa dampak – Cont'd

- ***Dampak atas Availability (Ketersediaan)***

  Kerugian ini menimbulkan dampak yang cukup signifikan terhadap misi organisasi karena terganggunya fungsionalitas sistem dan berkurangnya efektifitas operasional. Adapun hasil keluaran dari langkah ke 6 ini adalah kategorisasi dampak dari resiko dalam beberapa level seperti dijelaskan pada langkah 5 yang di implementasikan terhadap tingkat CIA tersebut di atas.

3. METODOLOGI PENILAIAN RESIKO

Langkah 7. Tahap Penentuan Resiko

Dalam tahap ini, dampak resiko didefinisikan dalam bentuk matriks sehingga resiko dapat terukur. Bentuk dari matriks tersebut dapat berupa matriks 4 x 4, 5 x 5 yang tergantung dari bentuk ancaman dan dampak yang di timbulkan.

3. METODOLOGI PENILAIAN RESIKO

Langkah 7. Tahap Penentuan Resiko – Cont'd

Probabilitas dari setiap ancaman dan dampak yang ditimbulkan dibuat dalam suatu skala misalkan probabilitas yang timbul dari suatu ancaman pada langkah ke 5 di skalakan dalam nilai 1.0 untuk tingkat Catastrophics, 0,7 untuk tingkat critical, 0,4 untuk tingkat marginal dan 0,1 untuk tingkat negligible.

3. METODOLOGI PENILAIAN RESIKO

Langkah 7. Tahap Penentuan Resiko – Cont'd

Adapun probabilitas dampak pada langkah ke 6 yang timbul di skalakan dalam 4 skala yang sama dengan nilai 4 dampak, dimana skala sangat tinggi di definisikan dalam nilai 100, tinggi dalam nilai 70, sedang diskalakan dalam penilaian 40 dan rendah diskalakan dalam nilai 10, maka matriks dari langkah ke 7 ini dapat di buat dalam bentuk :

3. METODOLOGI PENILAIAN RESIKO

Langkah 7. Tahap Penentuan Resiko – Cont'd

Tingkat Ancaman	Dampak			
	Sangat Tinggi (100)	Tinggi (70)	Sedang (40)	Rendah (10)
Catastrophic (1,0)	100 x 1= 100	70 x 1 = 70	40 x 1 = 40	10 x 1 = 10
Critical (0,7)	100 x 0,7 = 0,7	70 x 0,7 = 49	40 x 0,7 = 28	10 x 0,7 = 7
Marginal (0,4)	100 x 0,4 = 40	70 x 0,4 = 28	40 x 0,4 = 16	10 x 0,4 = 4
Negligible (0,1)	100 x 0,1 = 10	70 x 0,1 = 7	40 x 0,1 = 4	10 x 0,1 = 1

3. METODOLOGI PENILAIAN RESIKO

Langkah 8. Rekomendasi kontrol

Setelah langkah mendefinisikan suatu resiko dalam skala tertentu, langkah ke delapan ini adalah membuat suatu rekomendasi dari hasil matriks yang timbul dimana rekomendasi tersebut meliputi beberapa hal sebagai berikut :

1. Rekomendasi tingkat keefektifitasan suatu sistem secara keseluruhan
2. Rekomendasi yang berhubungan dengan regulasi dan undang-undang yang berlaku
3. Rekomendasi atas kebijakan organisasi
4. Rekomendasi terhadap dampak operasi yang akan timbul
5. Rekomendasi atas tingkat keamanan dan kepercayaan

Pendefinisian skala rekomendasi yang dibuat berdasarkan skala prioritas dari organisasi tersebut.

3. METODOLOGI PENILAIAN RESIKO

Langkah 9. Dokumentasi hasil pekerjaan

Langkah terakhir dari pekerjaan ini adalah pembuatan laporan hasil investigasi atas resiko bidang sistem informasi. Laporan ini bersifat laporan manajemen yang digunakan untuk melakukan proses mitigasi atas resiko di kemudian hari.