Manajemen Risiko TI

Magister Teknologi Informasi

Universitas Indonesia

Pengantar Risiko TI

Agenda

- Apa itu risiko TI?
- Bagaimana organisasi mengelola risiko TI?
- Konsep dasar manajemen risiko:
  - Definisi resiko dan manajemen risiko
  - Prinsip-prinsip dasar manajemen risiko
  - Siklus aktivitas proses manajemen risiko.

Manajemen Risiko TI

TATAKELOLA RISIKO TI

Risiko TI

- TI memainkan peran sentral dalam organisasi, sehingga dampak risiko TI terlalu besar untuk dapat diabaikan.
- Dampak insiden risiko TI:
  - Secara signifikan merugikan pihak-pihak terkait baik internal maupun eksternal (konsumen/ publik, rekanan, dsb.)
  - Merusak reputasi organisasi, tidak hanya manajemen TI tetapi manajemen organisasi secara umum.

Penyebab Risiko TI

- Mayoritas risiko TI bukan karena masalah teknis tetapi **kegagalan proses pengawasan dan tatakelola TI** organisasi: proses-proses pengambilan keputusan yang mengabaikan (sengaja atau tidak) potensi konsekuensi bisnis dari risiko TI.
- Kegagalan mengakibatkan rangkaian keputusan dan struktur aset TI yang bermasalah.
- Manifestasi kelemahan manajemen risiko TI:
  - Tatakelola TI yang tidak efektif
  - Kompleksitas yang tidak terkendali, dan
  - Kurangnya kesadaran terhadap risiko.

Kelemahan Tatakelola TI

- Tidak adanya struktur dan proses yang memungkinkan **keterlibatan pihak bisnis** dalam pengambilan keputusan tentang TI (termasuk investasi TI) berdampak:
  - **Keoptimalan keputusan** hanya diukur secara **lokal** (bagian/divisi/unit) untuk merespon kebutuhan lokal. Cepat atau lambat akan membatasi kelincahan organisasi untuk dapat tanggap terhadap kebutuhan bisnis (integrasi, layanan baru, dsb.)
  - Tanpa keterlibatan bisnis, pengambil keputusan TI dapat **salah dalam menilai tingkat risiko**. Berakibat pada prioritasi penerapan kontrol yang tidak tepat.

Kompleksitas Tak Terkendali

- Kompleksitas aset TI yang tinggi (bervariasi dan saling tumpang-tindih) meningkatkan kerawanan terhadap risiko
  - Rumit dan beratnya beban kerja pengelolaannya.
  - Keterbatasan SDM berkeahlian menimbulkan ketergantungan pada pihak ketiga.

Kurangnya Kesadaran terhadap Risiko

- Ketidak-pekaan terhadap **sumber risiko** TI:
  - Kelemahan dalam perencanaan SDM: mutasi, PHK, dan ketergantungan pada kontraktor pihak ketiga.
  - Kelemahan pengelolaan infrastruktur: digunakannya perangkat infrastruktur yang tidak handal.
  - Ketidak-tahuan dan ketidak-pedulian karyawan terhadap usaha menghindari resiko keamanan TI.
  - Tidak-adanya fasilitas (kontrol) untuk mendeteksi dan mencegah terjadinya aktivitas yang merugikan.

Menuju Lingkungan Peka Risiko

- Manajemen risiko TI adalah tanggung jawab bersama:
  - Pimpinan TI harus dapat menjelaskan kepada eksekutif bisnis tentang konsekuensi risiko TI.
  - Pimpinan TI harus menciptakan mekanisme pengambilan keputusan yang memungkinkan pembahasan risiko TI dari perspektif bisnis.
- Risiko TI bukan hanya masalah TI yang dipecahkan dengan teknologi dan keahlian pengelolaannya saja:
  - Inisiatif mitigasi risiko membutuhkan komitmen dari pimpinan organisasi, termasuk untuk berinvestasi dalam mengimplementasikan kontrol yang dibutuhkan.

Kemampuan Tatakelola Resiko TI

- Perusahaan yang mapan membangun kemampuan tatakelola risiko TI dengan:
  - Menerapkan kerangka-kerja terpadu dalam mengelola risiko TI sehingga dapat mengambil keputusan secara rasional dengan menimbang untung-ruginya dari perspektif bisnis
    - Adanya kesamaan persepsi terhadap risiko TI.
  - Menekankan pada **tiga pilar utama** manajemen resiko:
    1. *Penyederhanaan arsitektur TI*
    2. *Penerapan proses tatakelola risiko*, dan
    3. *Penciptaan budaya peka risiko*.

Manajemen Risiko TI

KONSEP MANAJEMEN RISIKO

Definisi Risiko dan Manajemennya

- **Risiko**
  - Kondisi atau kejadian (*event*) yang dapat berdampak positif atau negatif pada hasil suatu kegiatan.
  - Berbeda dengan problem, risiko adalah *potensi* (belum terjadi) timbulnya kerugian.
- **Manajemen Resiko**:
  - Proses identifikasi, analisa dan antisipasi risiko secara *proaktif*.
  - Tujuannya untuk memaksimalkan dampak positif (peluang) dan meminimalkan dampak negatif (kerugian).

Prinsip Dasar Manajemen Risiko

- **Bersifat *proaktif***:
  - Antisipatif, bukan reaktif
  - Mengatasi penyebab, bukan gejala
  - Menyiapkan rencana penanggulangan sebelum kejadiannya
  - Menerapkan prosedur penanggulangan yang baku
  - Menerapkan mekanisme *preventif* (mengurangi kemungkinan terjadinya) sejauh memungkinkan.
- **Bersifat *kolektif***: melibatkan setiap pihak (dengan bidang tanggung jawab masing-masing) dalam proses manajemen risiko.

Prinsip Dasar Manajemen Risiko

- **Bersifat *partisipatif***: secara terbuka membahas berbagai potensi risiko demi kesuksesan bersama untuk menghindari adanya risiko tersembunyi.
- **Bersifat *iteratif***: melalui siklus untuk memfasilitasi proses belajar (memahami risiko) dari pengalaman. Menjadikan evaluasi ulang risiko sebagai bagian dari siklus kegiatan.

Siklus Manajemen Risiko

- Siklus secara umum :

Identifikasi Risiko

- Merupakan aktivitas kolektif dengan sasaran tercapainya kesepakatan tentang daftar risiko yang dihadapi.
- Mempertimbangkan:
  - Pengalaman anggota tim
  - Pengetahuan umum tentang kategori dan jenis risiko:
    - *Operational, financial, technological*, dsb.
  - Kebijakan dan prosedur organisasi tentang manajemen risiko
  - Karakteristik kegiatan: konteks, tujuan, status pelaksanaan, catatan historisnya, dsb.

Pernyataan Risiko

- Setiap risiko dalam daftar resiko memiliki *risk statement* yang minimal mendefinisikan:
  - Penyebab (*root cause*)
  - Kondisi (atau *event*)
  - Akibat langsung (*consequence*) bagi kegiatan
  - Dampak (*downstream efect*) bagi bisnis

Analisa dan Prioritasi Risiko

- Karena keterbatasan sumber daya, risiko harus dianalisa untuk diprioritaskan mana yang utama harus ditanggulangi.
- Mempertimbangkan:
  - Pengalaman anggota tim
  - *Risk statement*
  - Pengetahuan tentang risiko tsb.
  - Kebijakan dan prosedur manajemen risiko organisasi
  - Penilaian pihak manajemen.

Analisa Risiko

- Menghitung derajad risiko (*risk exposure*) berdasarkan dua komponen:
  - Peluang terjadinya (*probability*)
  - Besarnya dampak (*impact*)
- Metoda penilaian *kualitatif* (semi kuantitatif) dan *kuantitatif*.
- *risk exposure* = *probability* x *impact*

Probabilitas

- Peluang terjadinya dapat diperkirakan berdasarkan:
  - Statistik terjadinya *event* (atau *event* serupa) pada masa lalu.
  - Perkiraan ahli di bidang terkait, dapat juga melalui konsensus anggota tim.
- Diukur secara kuantitatif atau semi-kuantitatif :

Probability range	Probability value used for calculations	Natural language expression	Numeric score
1% through 33%	17%	Low	1
34% through 67%	50%	Medium	2
68% through 99%	84%	High	3

Dampak

- Nilai kerugian yang diakibatkan, biasanya dalam nilai moneter (Rp, $, dsb.)
  - Sesuai dengan dampak dalam *risk statement*.
  - Termasuk: *opportunity cost, loss of market share, additional operational cost*, dsb.
- Dapat dinilai berdasarkan kriteria kasar, contoh:

Criterion	Cost overrun	Schedule	Technical
Low	Less than 1%	Slip 1 week	Slight effect on performance
Medium	Less than 5%	Slip 2 weeks	Moderate effect on performance
High	Less than 10%	Slip 1 month	Severe effect on performance
Critical	10% or more	Slip more than 1 month	Mission cannot be accomplished

Derajad Risiko

- Perkalian antara skor peluang kali skor dampak.
- Atau menggunakan matriks dengan daerah resiko:

Probability impact	Low = 1	Medium = 2	High = 3
High = 3	3	6	9
Medium = 2	2	4	6
Low = 1	1	2	3

- Contoh:
  - Rendah: 1-2, Sedang: 3-4, Tinggi: 6-9

Rencana Penanggulangan

- Penyusunan rencana untuk mengendalikan risiko-risiko dengan prioritas tinggi
  - Berupa implementasi mekanisme kontrol yang terintegrasi dalam prosedur kegiatan.
- Prinsip:
  - Kendalikan penyebab untuk memperkecil *probability*
  - Kendalikan akibat untuk memperkecil *impact*
  - Untuk risiko yang diluar wilayah kewenangan/ kendali, limpahkan ke pihajk yang berwenang.

Alternatif Tindakan

- *Accept*, terima jika masih dalam batas toleransi organisasi (*risk appetite*).
- *Avoid*, hindari dengan membatasi lingkup kegiatan.
- *Transfer*, alihkan kepada pihak lain termasuk dengan *outsourcing/subcontract/purchase* atau dengan asuransi.
- *Mitigate*, menerapkan mekanisme untuk menurunkan peluang terjadinya atau meminimalisasi dampaknya sampai batas yang dapat ditolerir.
- *Contingency*, menerapkan prosedur penanggulangan untuk meminimalkan dampak.

Pemantauan Risiko

- Memantau kerja mekanisme pengendalian risiko dengan:
  - Metrik indikator terjadinya risiko yang diukur dari aspek-aspek kinerja kegiatan (misalnya: kelambatan proses, peningkatan jumlah gangguan, jumlah pengerjaan ulang, dsb.)
- Mengaktifkan rencana *contingency* jika batas ambang terlampaui (*trigger*).

Kontrol/Penanggulangan

- Pelaksanaan *contingency plan* untuk mengendalikan dampak risiko yang telah terjadi
  - Misalnya aktivasi *Disaster Recovery Plan*.

Petik Pelajaran

- Sebagai mekanisme penyempurnaan proses manajemen risiko secara berkesinambungan
  - Memberikan umpan balik bagi proses manajemen risiko
  - Mencatat efektivitas identifikasi risiko (termasuk *scoring*, struktur, klasifikasi, dsb.) dan strategi mitigasi sebelumnya.
  - Mendokumentasikan pelajaran dalam suatu *risk knowledge base* yang dapat membantu proses identifikasi, analisa, dan perencanaan penanggulangan risiko di masa mendatang.