Analisis Resiko IT

Assoc.Prof. Dr. Muhammad Said Hasibuan,S.Kom.,M.Kom
Fakultas Ilmu Komputer IIB Darmajaya
2025

Definisi Resiko IT

- Risiko IT merujuk pada potensi kerugian atau dampak negatif yang dapat terjadi akibat penggunaan teknologi informasi dalam suatu organisasi.
- Ini mencakup berbagai ancaman, seperti serangan siber, kegagalan sistem, kehilangan data, dan pelanggaran privasi.
- Risiko ini dapat mempengaruhi integritas, kerahasiaan, dan ketersediaan informasi serta sistem yang mendukung operasi bisnis.

Pentingnya Resiko IT

Manajemen Risiko IT sangat penting karena:

1. **Perlindungan Aset**: Mengidentifikasi dan melindungi aset informasi penting dari ancaman yang dapat menimbulkan kerugian finansial atau reputasi.
2. **Kepatuhan Regulasi**: Memastikan bahwa organisasi mematuhi hukum dan regulasi yang berlaku terkait keamanan informasi dan perlindungan data.
3. **Pengambilan Keputusan yang Lebih Baik**: Memberikan dasar yang kuat untuk pengambilan keputusan terkait investasi teknologi dan strategi mitigasi risiko.
4. **Keberlanjutan Bisnis**: Meningkatkan ketahanan organisasi terhadap gangguan dan memastikan kelangsungan operasional dalam menghadapi insiden.

- .

Tujuan Analisis Risiko IT

Tujuan dari Analisis Risiko IT meliputi:

1. **Identifikasi Risiko**: Mengidentifikasi potensi risiko yang dapat mempengaruhi sistem dan data organisasi.
2. **Penilaian Risiko**: Mengevaluasi kemungkinan dan dampak dari risiko yang teridentifikasi untuk menentukan prioritas penanganan.
3. **Mitigasi Risiko**: Mengembangkan strategi untuk mengurangi atau mengelola risiko yang teridentifikasi, termasuk penerapan kontrol teknis dan administratif.
4. **Monitoring dan Review**: Memantau risiko secara berkelanjutan dan melakukan peninjauan berkala terhadap strategi manajemen risiko untuk menyesuaikan dengan perubahan dalam lingkungan bisnis dan teknologi.

Tujuan Analisis Risiko IT

Tujuan dari Analisis Risiko IT meliputi:

1. **Identifikasi Risiko**: Mengidentifikasi potensi risiko yang dapat mempengaruhi sistem dan data organisasi.
2. **Penilaian Risiko**: Mengevaluasi kemungkinan dan dampak dari risiko yang teridentifikasi untuk menentukan prioritas penanganan.
3. **Mitigasi Risiko**: Mengembangkan strategi untuk mengurangi atau mengelola risiko yang teridentifikasi, termasuk penerapan kontrol teknis dan administratif.
4. **Monitoring dan Review**: Memantau risiko secara berkelanjutan dan melakukan peninjauan berkala terhadap strategi manajemen risiko untuk menyesuaikan dengan perubahan dalam lingkungan bisnis dan teknologi.

FMEA

FMEA (Failure Modes and Effects Analysis) Analisis FMEA merupakan suatu teknik analisa bahaya secara kualitatif yang dapat digunakan untuk mengidentifikasi bagaimana suatu peralatan, fasilitas, atau sistem dapat gagal serta akibat yang dapat ditimbulkan (CCPS, 1992)

FMEA

Metode FMEA dilakukan untuk menganalisa potensibahaya/kegagalan pada setiap komponen sistem.

Potensi bahaya yang teridentifikasi akan dikelompokkan menurut besarnya potensi bahaya dan kemungkinan efek yang terjadi terhadap komponen sistem.)

FMEA

Hasil dari identifikasi bahaya menggunakan metode FMEA yaitu berupa nilai RPN (Risk Priority Number), kemudian akan diketahui komponen mana yang memiliki nilai RPN paling tinggi.

Tujuan dan Manfaat FMEA

a. Untuk mengidentifikasi mode kegagalan dan tingkat keparahan dampaknya.
b. Untuk mengidentifikasi karakteristik kritis dan signifikan.
c. Untuk mengurutkan pesanan desain potensial dan definisi proses.
d. Mengidentifikasi defisiensi proses, sehingga para engineer dapat berfokus pada pengendalian untuk mengurangi output sistem yang tidak sesuai dengan yang diinginkan atau pada metode untuk meningkatkan deteksi pada produk yang tidak sesuai tersebuti.

Identifikasi FMEA

FMEA dilakukan identifikasi penilaian risiko atau Risk Priority Number (RPN) terhadap sistem E-Recruitment yang bertujuan untuk mengetahui tingkat risiko bahaya yang paling kritis dengan memperhatikan risiko yang memiliki tingkat keparahan yang tinggi dan memiliki dampak atau keparahan yang besar serta kemampuan deteksi untuk mencegah terjadinya dampak yang ditimbulkan.

Nilai RPN didapatkan melalui hasil perkalian antara severity (S), occurance (O), dan detection (D)

Identifikasi FMEA

Tabel 1. Tingkat Dampak / Keparahan (Severity (S))

Rank	*Severity*	Deskripsi
10	Berbahaya tanpa peringatan	Kegagalan sistem yang menghasilkan efek sangat berbahaya
9	Berbahaya dengan peringatan	Kegagalan sistem yang menghasilkan efek berbahaya
8	Sangat tinggi	Sistem tidak beroperasi
7	Tinggi	Sistem beroperasi tetapi tidak dapat dijalankan secara penuh
6	Sedang	Sistem beroperasi dan aman tetapi mengalami penurunan performa sehingga mempengaruhi *output*
5	Rendah	Mengalami penurunan kinerja secara bertahap
4	Sangat rendah	Efek yang kecil pada performa sistem
3	Kecil	Sedikit berpengaruh pada kinerja sistem
2	Sangat kecil	Efek yang diabaikan pada kinerja sistem
1	Tidak ada efek	Tidak ada efek

Identifikasi FMEA

Tabel 2. Tingkat kemungkinan kejadian (*Occurrence*)

Rank	*Occurrence*	Deskripsi
10	Sangat tinggi	≥ 1 kejadian / shift
9		≥ 1 kejadian / hari
8	Tinggi	≥ 1 kejadian / 2-3 hari
7		≥ 1 kejadian / minggu
6	Sedang	≥ 1 kejadian / 2 minggu
5		≥ 1 kejadian / bulan
4	Rendah	≥ 1 kejadian / 4 bulan
3		≥ 1 kejadian / ½ tahun
2	Tidak ada efek	≥ 1 kejadian / tahun
1		≥ 1 kejadian / > 1 tahun

Identifikasi FMEA

Tabel 2. Tingkat kemungkinan kejadian (*Occurrence*)

Rank	*Occurrence*	Deskripsi
10	Sangat tinggi	≥ 1 kejadian / shift
9		≥ 1 kejadian / hari
8	Tinggi	≥ 1 kejadian / 2-3 hari
7		≥ 1 kejadian / minggu
6	Sedang	≥ 1 kejadian / 2 minggu
5		≥ 1 kejadian / bulan
4	Rendah	≥ 1 kejadian / 4 bulan
3		≥ 1 kejadian / ½ tahun
2	Tidak ada efek	≥ 1 kejadian / tahun
1		≥ 1 kejadian / > 1 tahun

Identifikasi FMEA

Tabel 3. Tingkat Deteksi Penyebab (*Detection* (D))

Rank	*Detection*	Deskripsi
10	Tidak pasti	Pengecekan akan selalu tidak mampu untuk mendeteksi penyebab kegagalan.
9	Sangat kecil	Pengecekan memiliki kemungkinan *very remote* untuk mampu mendeteksi penyebab kegagalan.
8	Kecil	Pengecekan memiliki kemungkinan "*remote*" untuk mampu mendeteksi penyebab kegagalan.
7	Sangat rendah	Pengecekan memiliki kemungkinan sangat rendah untuk mampu mendeteksi penyebab kegagalan.
6	Rendah	Pengecekan memiliki kemungkinan rendah untuk mampu mendeteksi penyebab kegagalan.
5	Sedang	Pengecekan memiliki kemungkinan "*moderate*" untuk mendeteksi penyebab kegagalan.
4	Menengah keatas	Pengecekan memiliki kemungkinan "*moderate high*" untuk mendeteksi penyebab kegagalan.
3	Tinggi	Pengecekan memiliki kemungkinan tinggi untuk mendeteksi penyebab kegagalan.
2	Sangat tinggi	Pengecekan memiliki kemungkinan sangat tinggi untuk mendeteksi penyebab kegagalan.
1	Hampir pasti	Pengecekan akan selalu mendeteksi penyebab kegagalan.

Identifikasi FMEA

Tabel 3. Tingkat Deteksi Penyebab (*Detection* (D))

Rank	*Detection*	Deskripsi
10	Tidak pasti	Pengecekan akan selalu tidak mampu untuk mendeteksi penyebab kegagalan.
9	Sangat kecil	Pengecekan memiliki kemungkinan *very remote* untuk mampu mendeteksi penyebab kegagalan.
8	Kecil	Pengecekan memiliki kemungkinan "*remote*" untuk mampu mendeteksi penyebab kegagalan.
7	Sangat rendah	Pengecekan memiliki kemungkinan sangat rendah untuk mampu mendeteksi penyebab kegagalan.
6	Rendah	Pengecekan memiliki kemungkinan rendah untuk mampu mendeteksi penyebab kegagalan.
5	Sedang	Pengecekan memiliki kemungkinan "*moderate*" untuk mendeteksi penyebab kegagalan.
4	Menengah keatas	Pengecekan memiliki kemungkinan "*moderate high*" untuk mendeteksi penyebab kegagalan.
3	Tinggi	Pengecekan memiliki kemungkinan tinggi untuk mendeteksi penyebab kegagalan.
2	Sangat tinggi	Pengecekan memiliki kemungkinan sangat tinggi untuk mendeteksi penyebab kegagalan.
1	Hampir pasti	Pengecekan akan selalu mendeteksi penyebab kegagalan.

Identifikasi FMEA

Tabel 4. Skala Pengukuran Pernyataan

Ukuran Pernyataan	Bobot Nilai
Sangat setuju/ Sangat tinggi/ Sangat banyak/ Selalu	5
Setuju/ Tinggi/ Banyak/ Sering	4
Netral/ Kadang-kadang/ Cukup	3
Tidak setuju/ Rendah/ Sedikit/ Hampir tidak pernah	2
Sangat tidak setuju/ Sangat rendah/ Sangat sedikit/ Tidak pernah	1

Terima Kasih