Institut Informatika & Bisnis
DARMAJAYA
Yayasan Alfian Husin

4

METODE DAN ALAT MANAJEMEN RISIKO KEAMANAN INFORMASI

National Institute of Standards and Technology (NIST) 800-30

- NIST 800-30 pertama kali dipublikasikan pada tahun 2002 oleh National Institute of Standards and Technology.
- Standar ini merupakan publikasi khusus mengenai Risk Guide for Information Technology System yang menyediakan 30 dasar untuk pengembangan program manajemen risiko yang efektif.
- Dapat digunakan untuk menilai dan memitigasi risiko yang teridentifikasi di dalam suatu sistem teknologi informasi karena mengandung definisi-definisi dan arahan praktis yang dibutuhkan.

Tujuan NIST 800-30

Untuk membantu organisasi dalam mengelola risiko teknologi informasi menjadi lebih baik.

Kerangka kerja ini menyediakan informasi dengan menyeleksi kontrol keamanan informasi yang efektif secara biaya sehingga dapat digunakan untuk memitigasi risiko untuk memberikan perlindungan bagi informasi penting, sistem informasi, dan pembawa informasi tersebut.

3 Aktivitas Proses Manajemen Risiko NIST 800-30

Sumber: Stoneburner, 2002

Penilaian Risiko NIST 800-30

- Organisasi menentukan ancaman dan risiko potensial terkait dengan sistem teknologi informasi menggunakan penilaian risiko.
- Melakukan identifikasi, evaluasi dan efek risiko, serta rekomendasi untuk pengukuran pengurangan risiko.
- Terdapat 9 langkah dalam penilaian risiko

Penilaian Risiko NIST 800-30

Terdapat 9 langkah dalam penilaian risiko

1. *System Characterization,* dalam menilai risiko, perlu ditentukan ruang lingkup dari sistem yang akan dinilai. pad tahap ini dilakukan juga identifikasi berbagai batasan dari sistem serta sumberdaya dan informasi yang berkaitan dengan sistem.
2. *Threat Identification,* mengidentifikasi sumber ancaman dan hal-hal lain yang menjadi penyebab terjadinya ancaman. Penyebab terjadinya ancaman bisa diakibatkan adanya masalah internal ataupun ekternal.
3. *Vulnerability Identification*, tahap ini dilakukan identifikasi sumber kerentanan serta hal yang menjadi penyebab terjadinya ancaman. Kerentanan bisa terjadi di dalam perancangan, implementasi, prosedur keamanan sistem, atau kontrol internal yang dapat disalahgunakan.
4. *Control Analysis,* setiap kontrol yang telah atau akan diimplementasikan perlu untuk dilakukan analisis untuk mengurangi kemungkinan terjadinya ancaman.
5. *Likehood Determination*, menentukan tingkatan dari probabilitas suatu kelemanan dapat disalahgunakan oleh sumber ancaman. tingkatan ini dibagi menjadi 3 yaitu *High, Medium*, dan *Low.*

Penilaian Risiko NIST 800-30

Terdapat 9 langkah dalam penilaian risiko

6. *Impact Analysis,* dampak dari kelemahan yang disalahgunakan dapat dianalisis dengan mengacu pada tingkat kepentingan sistem dan data, misi sistem, dan tingkat sensitivitas sistem dan data. Hasil dari tahap ini dapat dinyatakan dalam 3 tahap tingkatan yaitu *High, Medium*, dan *Low.*
7. *Risk Determination,* pada tahap ini dilakukan penilain tingkat risiko pada sistem teknologi informasi. Skala dari risiko dan matrik dari level risiko digunakan untuk melakukan penilaian. Hasil dari tahap ini dapat dinyatakan dalam 3 tahap tingkatan yaitu *High, Medium*, dan *Low.*
8. *Control Recommendation,* dua langkah terakhir adalah dengan menetukan rekomendasi dari kontrol resiko yang relevan dengan aktivitas organisasi dimana dapat digunakan untuk memitigasi atau menghilangkan risiko yang teridentifikasi. Hal ini bertujuan untuk menurunkan tingkat risiko sistem informasi dan datanya ke tingkat yang lebih baik atau dapat diterima.
9. *Results Documentation*, langkah terakhir merupakan dokumentasikan hasil dari keseluruhan tahap.

Mitigasi Risiko NIST 800-30

Metodologi mitigasi resiko yang dilakukan dalam proses mitigasi:

1. *Prioritize Action,* langkah awal ini dilakukan untuk menentukan prioritas dari kegiatan yang akan diimplementasikan berdasarkan level risiko yang didapat dari penilaian risiko. Hasil dari tahapan ini adalah urutan prioritas kegiatan dari yang tertinggi hingga terendah.
2. *Evaluate Recommended Control Options,* pada tahap ini dilakukan analisis terhadap efektivitas dari rekomendasi kontrol dengan tujuan untuk memilih kontrol yang sesuai dan berhubungan agar dapat mengurangi risiko.
3. *Conduct Cost-Benefit Analysis,* Pada tahap ini dilakukan analisis *cost-benefit* dari rekomendasi kontrol yang digunakan untuk membantu pihak manajemen dalam membuat keputusan kontrol apa saja yang akan digunakan dengan melihat kontrol yang memiliki biaya lebih efektif.

Mitigasi Risiko NIST 800-30

Metodologi mitigasi resiko yang dilakukan dalam proses mitigasi:

4. *Select Control,* setelah dilakukan analisis biaya, langkah selanjutnya yaitu memilih kontrol-kontrol yang akan dipakai dengan menggabungkan aspek operasional, kontrol manajemen, dan teknis untuk memastikan keamanan sistem teknologi informasi dan keamanan perusahaan.
5. *Assign Responsibility*, Orang-orang yang tepat (personel in-house atau staf kontraktor eksternal) yang memiliki keahlian dan keterampilan yang tepat untuk melaksanakan kontrol yang dipilih diidentifikasi, dan bertanggung jawab dengan tugasnya.
6. *Develop a Safeguard Implementation Plan*, Dalam tahap ini dilakukan pengembangan suatu *action plan* yang terdiri dari informasi mengenai risiko, rekomendasi kontrol, prioritas kegiatan, kontrol yang dipilih, sumber daya yang dperlukan, daftar tanggung jawab personil dan tim, tanggal mulai dan selesainya implementasi, dan kebutuhan pemeliharaan.
7. *Implement Selected Controls,* pada tahap akhir ini implementasi kontrol yang dipilih telah dilakukan.

Evaluating Risiko **NIST 800-30**

- Di sebagian besar organisasi, jaringan akan terus diperluas dan diperbarui, komponennya berubah, dan aplikasi perangkat lunaknya diganti atau diperbarui dengan versi yang lebih baru.
- Selain itu, perubahan personel akan terjadi dan kebijakan keamanan cenderung berubah seiring waktu.
- Perubahan-perubahan ini berarti bahwa risiko-risiko baru akan muncul dan risiko-risiko yang sebelumnya dikurangi dapat kembali menjadi perhatian.
- Dengan demikian, proses manajemen risiko sedang berlangsung dan berkembang.
- Praktik yang baik dan kebutuhan untuk evaluasi dan penilaian risiko yang berkelanjutan dan faktor-faktor yang akan mengarah pada program manajemen risiko yang sukses.

Failure Model Effect Analysis (FMEA)

FMEA adalah teknologi yang dirancang untuk mengidentifikasi mode kegagalan potensial pada suatu proses sebelum terjadi, dengan mempertimbangkan risiko yang berkaitan dengan mode kegagalan tersebut serta efeknya

Failure Model Effect Analysis (FMEA)

FMEA dapat dilakukan dengan cara:

1. Mengenali dan mengevaluasi kegagalan potensi suatu produk dan efeknya
2. Mengidentifikasi tindakan yang bisa menghilangkan atau mengurangi kesempatan dari kegagalan potensi terjadi
3. Pencatatan proses sehingga dokumen perlu di *update* secara teratur agar dapat digunakan untuk mencegah dan mengantisipasi terjadinya kegagalan

Penilaian FMEA

Severity (tingkat keparahan).

- *Severity* atau keseriusan efek kegagalan merupakan pengukurandalam memperkirakan subjektif numeric dari seberapa parah efek kegagalan yang akan dirasakan oleh pengguna akhir.
- Ukuran parameter dari *severity* berperingkat dari angka 1 sampai dengan 10 (Tidak ada(none) sampai dengan Berbahaya; tanpa peringatan)

Penilaian FMEA

Occurance (kemungkinan terjadi kesalahan)

- *Occurance* atau frekuensi kegagalan merupakan pengukuran dalam memperkirakan subjektif numerik dari probabilitas penyebab kemungkinan terjadinya kegagalan akanmenghasilkan mode kegagalan yang menyebabkan akibat tertentu.
- Ukuran parameter dari *Occurance* berperingkat dari angka 1 sampai dengan 10 (***Hampir tidak mungkin :*** **Hampir tidak mungkin terjadi** sampai dengan ***Sangat tinggi*** **– kegagalan hampir tak terelakan**)

Penilaian FMEA

Detection (deteksi tiap kesalahan)

- *Detection* atau sejauh mana peluang potensi kegagalan tersebut dapat teridentifikasi merupakan pengukuran dalam memperkirakan subjektif numerik dari kontrol untuk mencegah atau mendeteksi penyebab kegagalan sebelum kegagalan mencapai pengguna akhir atau pelanggan.
- Ukuran parameter dari *Detection* berperingkat dari angka 1 sampai dengan 10 (*Hampir pasti – terlihat jelas sangat mudah pengendaliannya* sampai dengan *Hampir tidak mungkin – Potensi penyebab tidak terdeteksi*)

Penilaian FMEA

Risk Priority Number (RPN)

RPN adalah hasil ukuran yang digunakan ketika menilai risiko untuk membantu mengidentifikasi *critical failure modes* atau mode kegagalan kritis terkait dengan suatu sistem mencakupi desain atau proses. Nilai RPN berkisar dari 1(terbaik mutlak) hingga 1000 (absolut terburuk).

- Severity (S)
- Severity X Occurrence (S X O)
  - Criticality
- Severity X Occurrence X Detection (S X O X D) = RPN

Rumus Penilaian RPN

CLASS OF RPN CATAGORISM	
RPN Calculation	Level
< 20	Very Low
< 80	Low
< 120	Medium
< 200	High
>200	Very High

Klasifikasi level risiko berdasarkan RPN