RISK (RISIKO)

TKB7351 - Keamanan Informasi & Jaringan
TKB7358 - Keamanan Sistem Informasi

Chalifa Chazar
http://script.id
chalifa.chazar@gmail.com

- Keamanan informasi diperoleh dengan mengimplementasikan berbagai kontrol dan kebijakan
- Langkah awal untuk menetapkan kebijakan keamanan adalah dengan mempelajari, mengevaluasi semua resiko yang muncul akibat penggunaan sistem

Jenis Informasi

- Arsip elektronik
- Dokumen dalam bentuk kertas
- Rekaman
- Komunikasi

- Secara umum, resiko selalu berkaitan dengan bisnis organisasi
- Merupakan proses yang komplek karena menyangkut masalah biaya

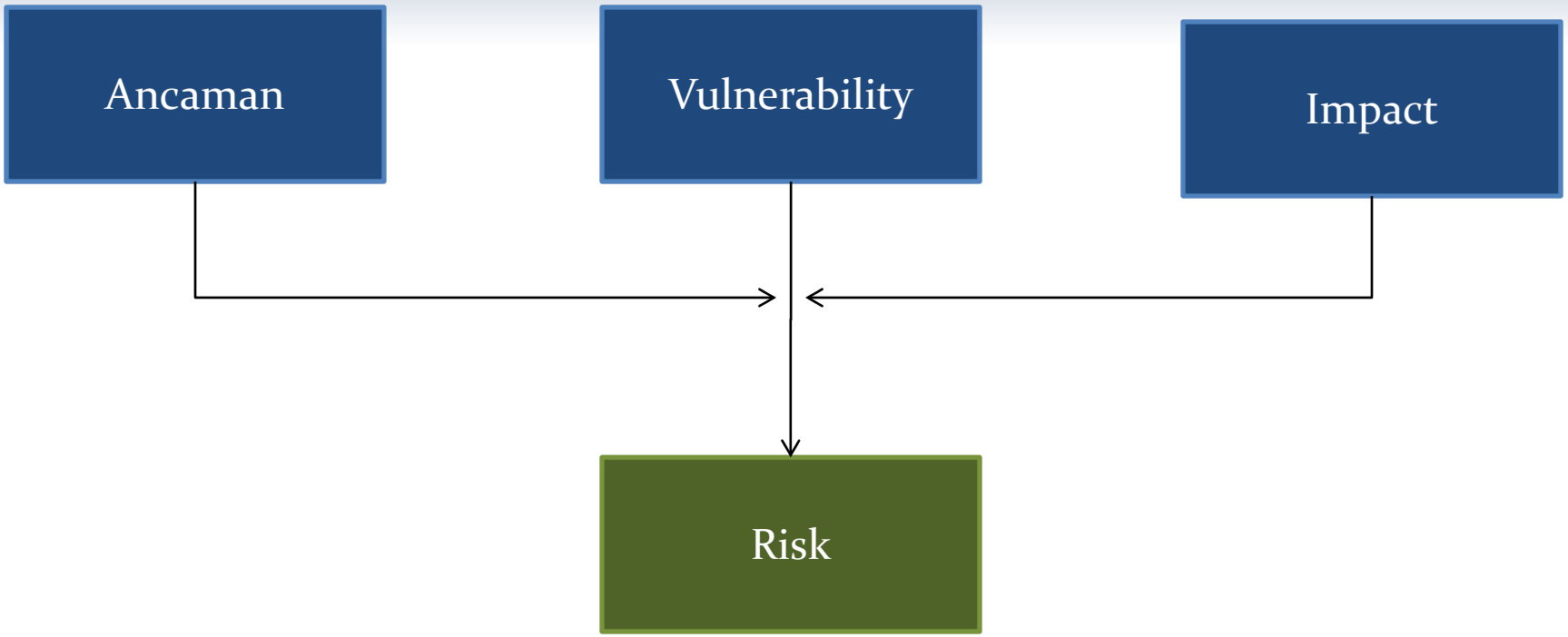
Risk

- Resiko merupakan kombinasi dari komponen kejadian yang menyangkut:
  - Ancaman (*threat)*
  - *Vulnerability*
  - *Impact*

- **Ancaman keamanan sistem** = aksi yang terjadi baik dalam sistem maupun diluar sistem yang dapat mengganggu keseimbangan SI
- **Vulnerability=** kelemahan keamanan sistem sebagai penunjang bisnis perusahaan yang dapat dimanfaatkan oleh pihak lain untuk menguasai sistem yang bersangkutan
- **Impact=** penilaian atas pengaruh ancaman yang dilakukan terhadap aset maupun tujuan organisasi dengan memanfaatkan kelemahan sistem

Jenis Impact

- Kerugian atas *revenue*
- Kerugian atas modal oraganisasi
- Kerusian mengenai reputasi pasar
- Hilangnya *business opportunity*
- Kerugian pasar modal
- Kehilangan kepercayaan pelanggan, karyawan, pemegang saham
- Pelanggaran regulasi dan hukum
- Tercemarnya nama baik organisasi


Ancaman
Vulnerability
Impact
Risk

Risk analysis

- *Risk analysis* merupakan cikal bakal pembuatan kebijakan keamanan sistem dari organisasi

- Sebelum membuat kebijakan keamanan sistem, perlu mengidentifikasi sumber daya yang ada

Risk analysis (2)

- Apa yang harus diproteksi dan dikontrol oleh organisasi?
- Apa yang dibutuhkan untuk memproteksinya?
- Bagaimana cara memproteksi dan mengontrolnya?
- Prioritas

Tujuan Risk Assesment

- Mengidentifikasi proteksi dan kontrol terhadap informasi

- Kontrol terhadap sistem informasi tidak boleh mengabaikan tujuan/misi bisnis organisasi

- Tujuan utama proteksi terhadap informasi adalah menciptakan lingkungan yang aman dan terjamin bagi manajemen untuk melakukan tugasnya

- Faktor yang ikut dipertimbangkan adalah peraturan pemerintah yang berhubungan

- Resiko dikelompokan oleh tingkat kepentingan dan dampak kerusakan yang diakibatkannya

- Faktor penentunya:
  - Perkiraan resiko kehilangan sumber daya (sengaja atau tidak sengaja)
  - Perkiraan pentingnya sumber daya (apa *impact-nya)*

Kategori sumber daya yg dipertimbangkan

- Hardware
- Software
- Data
- Manusia
- Dokumentasi
- Persediaan

</THANKS>

Chalifa Chazar
http://script.id
Email: chalifa.chazar@gmail.com