RISK (RISIKO)

TKB4364 - Keamanan Informasi & Jaringan

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

Last update : Januari 2022 | chalifa.chazar@gmail.com

- Keamanan informasi diperoleh dengan mengimplementasikan berbagai kontrol dan kebijakan
- Langkah awal untuk menetapkan kebijakan keamanan adalah dengan mempelajari, mengevaluasi semua risiko yang muncul akibat penggunaan system
- Risiko selalu berkaitan dengan bisnis organisasi dan merupakan proses yang komplek karena menyangkut masalah biaya

Jenis Informasi

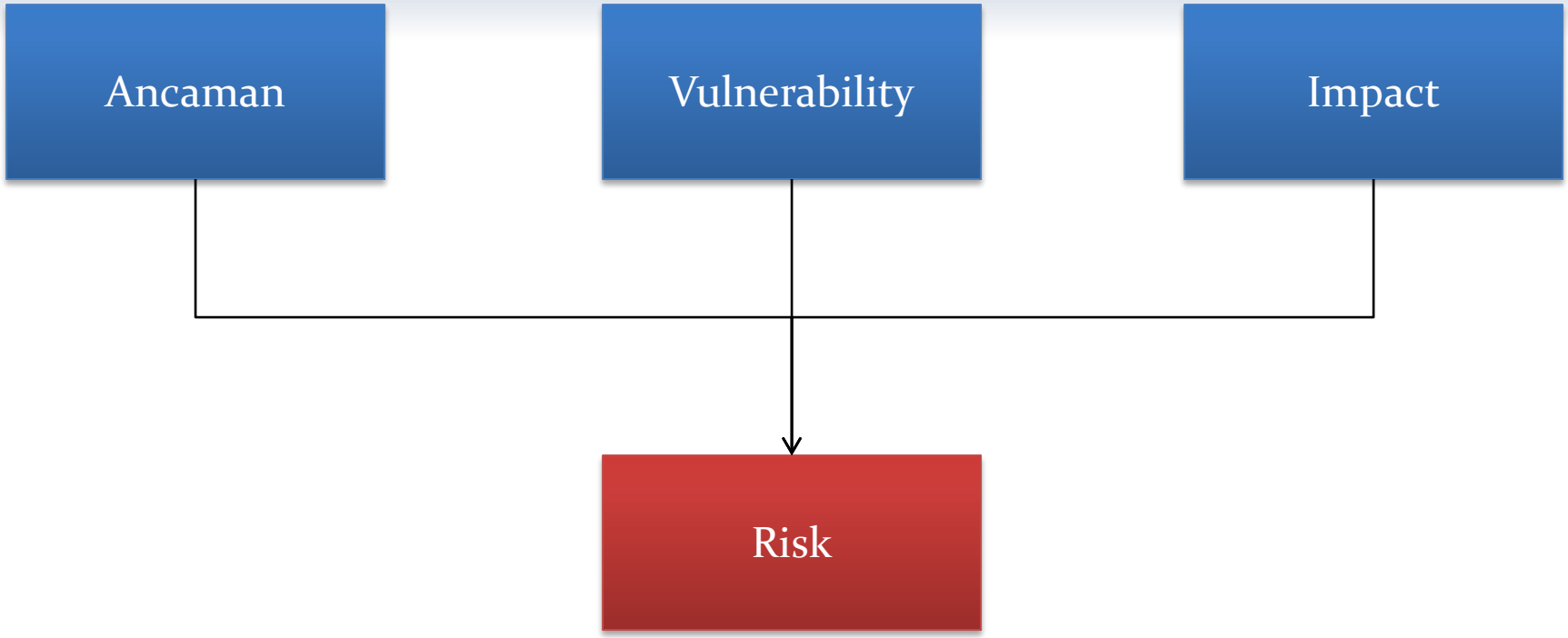
- Arsip bentuk fisik (hardcopy)
- Penyimpanan secara digital (cloud)
- Visual (video, diagram)
- Informasi dalam website
- Rekaman (cctv, hasil citra digital)
- Komunikasi (vebal percakapan, panggilan telepon)

Risiko

- Risiko (risk) merupakan **kombinasi** dari komponen kejadian yang menyangkut:
  - **Ancaman (threat)**
  - **Kelemahan (vulnerability)**
  - **Dampak (impact)**

- **Ancaman** = aksi yang terjadi baik dalam sistem maupun diluar sistem yang dapat mengganggu keseimbangan Sistem Informasi
- **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

Hubungan Keterkaitan



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

Risk analysis

- Risk analysis merupakan cikal bakal pembuatan kebijakan keamanan sistem dari organisasi atau dikenal juga sebagai risk managemen
- Sebelum membuat kebijakan keamanan sistem, perlu mengidentifikasi sumber daya yang ada
- Framework untuk risk management diantaranya **NIST** (The National Institute of Standard and Technology) dan **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

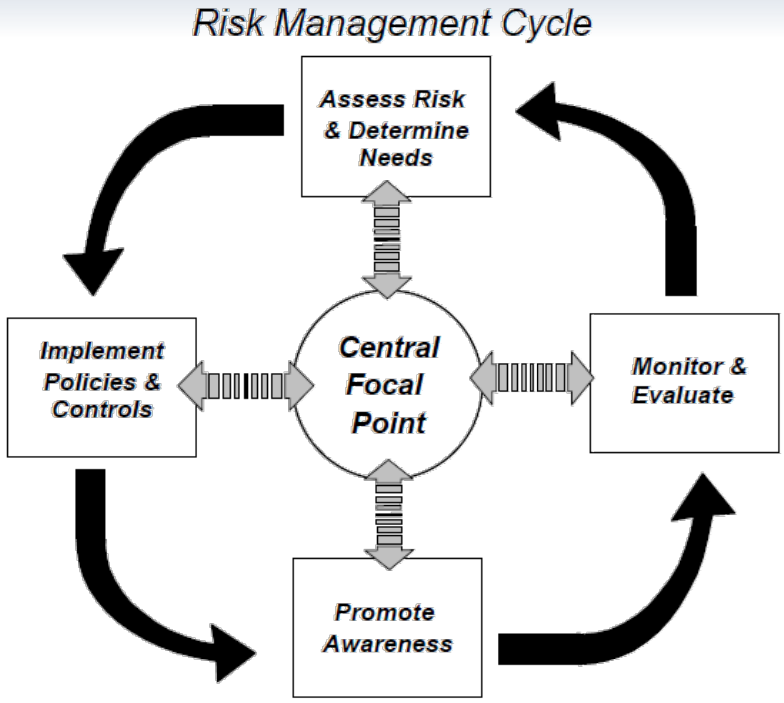
Risk analysis

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

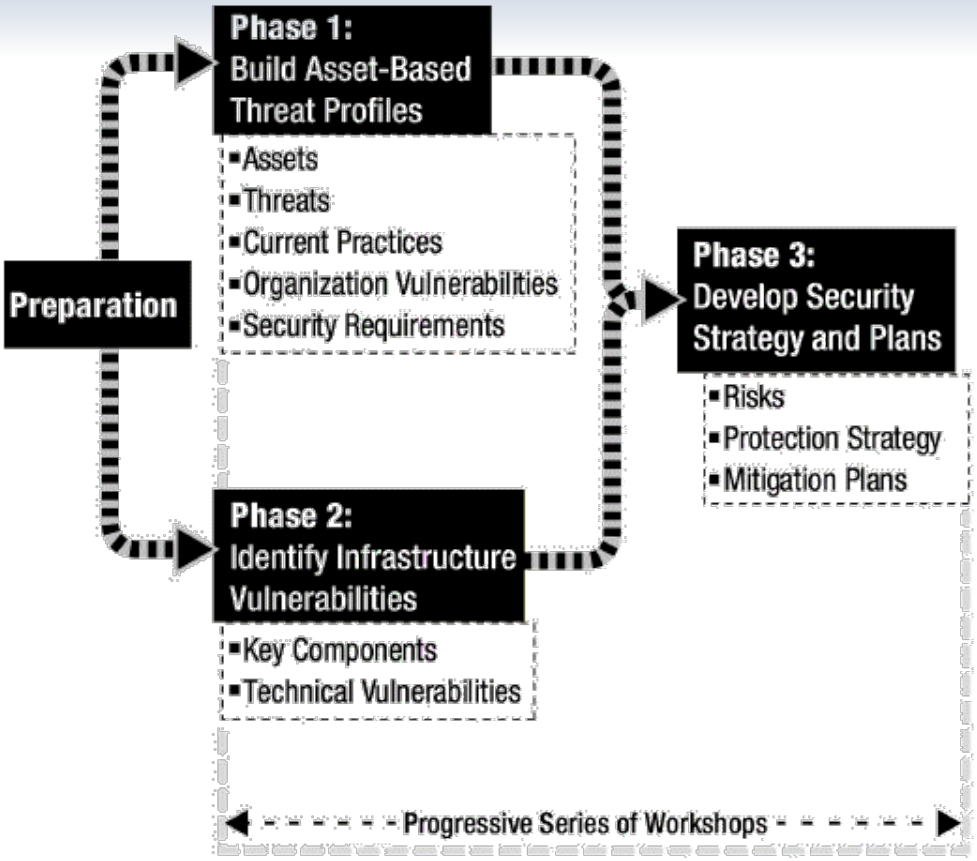
NIST

Risk Management Principles Implemented by Leading Organizations

- Assess risk and determine needs
- Establish a central management focal point
- Implement appropriate policies and related controls
- Promote awareness
- Monitor and evaluate policy and control effectiveness



OCTAVE


Phase 1:
Build Asset-Based
Threat Profiles
▪Assets
▪Threats
▪Current Practices
▪Organization Vulnerabilities
▪Security Requirements
Preparation
Phase 3:
Develop Security
Strategy and Plans
▪Risks
▪Protection Strategy
▪Mitigation Plans
Phase 2:
Identify Infrastructure
Vulnerabilities
▪Key Components
▪Technical Vulnerabilities
Progressive Series of Workshops

Tujuan Manajemen Risiko (ISO 31000:2018)

- Menekankan tujuan manajemen risiko, yaitu menciptakan dan melindungi nilai.
- Tujuan itu diwujudkan dengan (1) meningkatkan kinerja, (2) mendorong inovasi, dan (3) mendukung pencapaian sasaran
- Manajemen risiko adalah bagian dari tata kelola (governance) dan harus terintegrasi di dalam proses organisasi

Risk Assessment

- Capaian dari risk management adalah kebijakan strategi keamanan dan rencana mitigasi risiko (risk mitigation plans)
- Setiap kebijakan strategi perlu dinilai melalui proses risk assessment
- Risk Assessment (penilaian risiko) adalah merupakan suatu aktivitas yang dilaksanakan untuk memperkirakan suatu risiko dari situasi yang bisa didefinisikan dengan jelas ataupun potensi dari suatu ancaman atau bahaya baik secara kuantitatif atau kualitatif

Risk Assessment

- Risk Assessment bertujuan mengidentifikasi proteksi dan kontrol terhadap informasi, perlu diperhatikan bahwa kontrol terhadap sistem informasi tidak boleh mengabaikan tujuan atau visi-misi bisnis organisasi
- Proteksi terhadap informasi adalah menciptakan lingkungan yang aman dan terjamin bagi manajemen untuk melakukan tugasnya
- Faktor yang ikut dipertimbangkan adalah peraturan pemerintah yang berhubungan

Penilaian Risiko

- Risiko dikelompokan oleh tingkat kepentingan dan dampak kerusakan yang diakibatkannya
- Faktor penentunya:
  - Perkiraan risiko kehilangan sumber daya (sengaja atau tidak sengaja)
  - Perkiraan pentingnya sumber daya (apa impact-nya)

Dalam menilai suatu risiko terdapat standard yang bisa dipakai acuan, salah satunya ialah standard AS/NZS 4360 yang membuat peringkat risiko sebagai berikut:

- E : Extreme Risk (Sangat berisiko segera secepatnya dibutuhkan tindakan)
- H : High Risk (Risiko yang besar dibutuhkan perhatian dari manajer puncak)
- M : Moderat Risk (Risiko sedang, diibutuhkan sebuah tinggakan agar risiko berkurang)
- L : Low Risk (Risiko rendah masih ditoleransi)

Tugas 2

- Pada tugas sebelumnya, Anda diminta untuk mengidentifikasikan asset dan juga ancaman terhadap asset tersebut
- Selanjutnya, buat sebuah strategi kebijakan terhadap ancaman asset-asset tersebut

</THANKS>

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