Konsep Pengukuran saat Resiko Terjadi (At Risk)

Risk Assessment Menggunakan Metode OCTAVE

- Risk Assessment
- Metode OCTAVE
- Tahapan OCTAVE
- Perbedaan OCTAVE - OCTAVE/S – OCTAVE Alegro

Risk Assessment

Risk assessment memegang peranan penting dalam penerapan sistem manajemen keamanan informasi. Ada banyak metode yang dapat digunakan untuk melaksanakan risk assessment, karena banyaknya konsultan keamanan informasi yang mengembangkan berbagai pendekatan untuk melakukannya. Satu yang terkenal diantaranya adalah metode OCTAVE yang dikembangkan oleh Carnegie Mellon Software Engineering Institute, Pittsburg.

Metode OCTAVE

Metode OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation) yang dikembangkan Software Engineering Institute, Carnegie Mellon University, 1999 adalah sebuah pendekatan terhadap evaluasi risiko keamanan informasi yang komprehensif, sistematik, terarah, dan dilakukan sendiri.

Pendekatannya disusun dalam satu set kriteria yang mendefinisikan elemen esensial dari evaluasi risiko keamanan informasi.

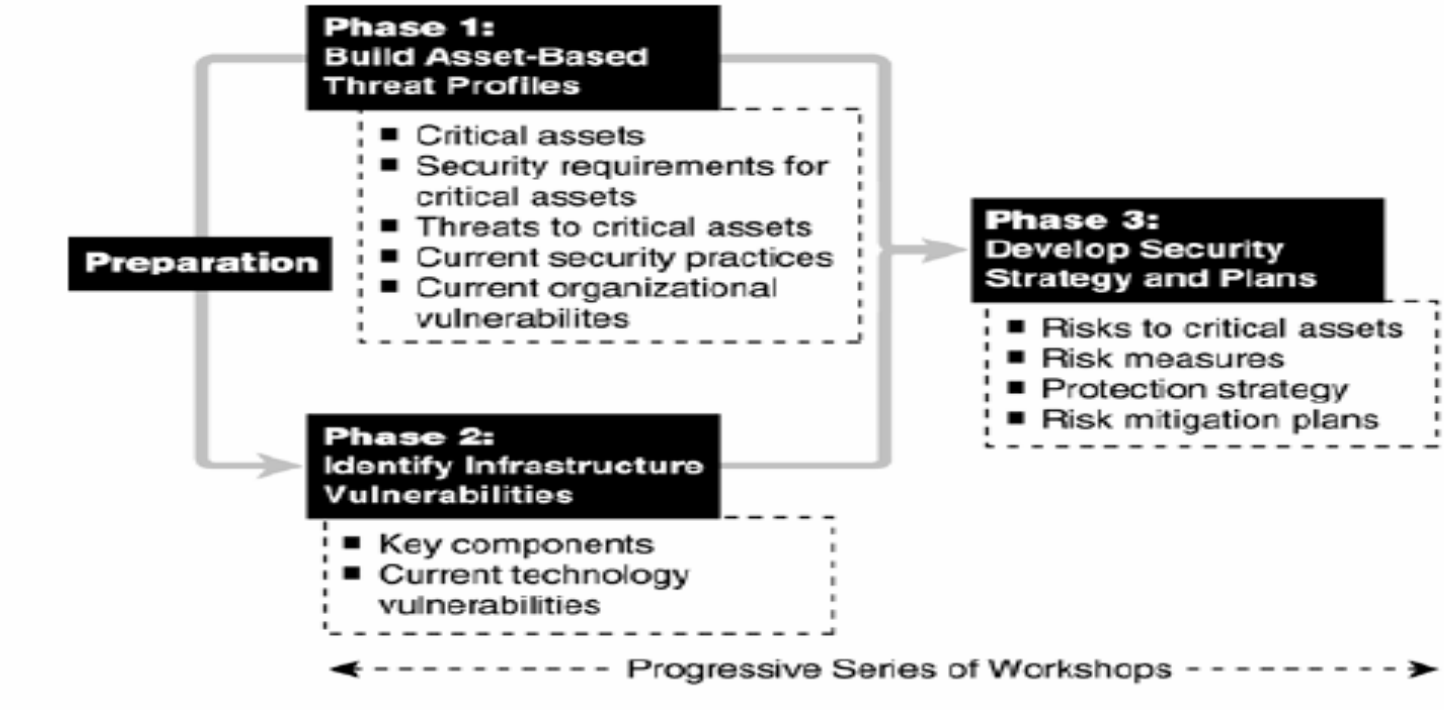
Kriteria OCTAVE memerlukan eveluasi yang harus dilakukan oleh sebuah tim interdisipliner yang terdiri dari personil teknologi informasi dan bisnis organisasi.

Anggota tim bekerjasama untuk membuat keputusan berdasarkan risiko terhadap aset informasi kritis organisasi.

Kriteria OCTAVE memerlukan katalog informasi untuk mengukur praktek organisasi, menganalisa ancaman, dan membangun strategi proteksi dan catalog ini menjadikan sumber database pengetahuan.

Katalog ini meliputi:

- ***catalog of practices*** → sebuah koleksi strategi dan praktek keamanan informasi.
- ***generic threat profile*** → sebuah koleksi sumber ancaman secara umum.
- ***catalog of vulnerabilities*** → sebuah koleksi dari kelemahan berdasarkan platform dan aplikasi



Gambar 1. Metode OCTAVE

Dengan menggunakan pendekatan tiga tahapan, metode OCTAVE menguji isu-isu organisasi dan teknologi terhadap penyususnan masalah-masalah yang komprehensif berdasarkan kebutuhan keamanan informasi sebuah organisasi.

Tahapan OCTAVE

1. Tahap 1 : Membangun Aset Berbasis Ancaman Profil

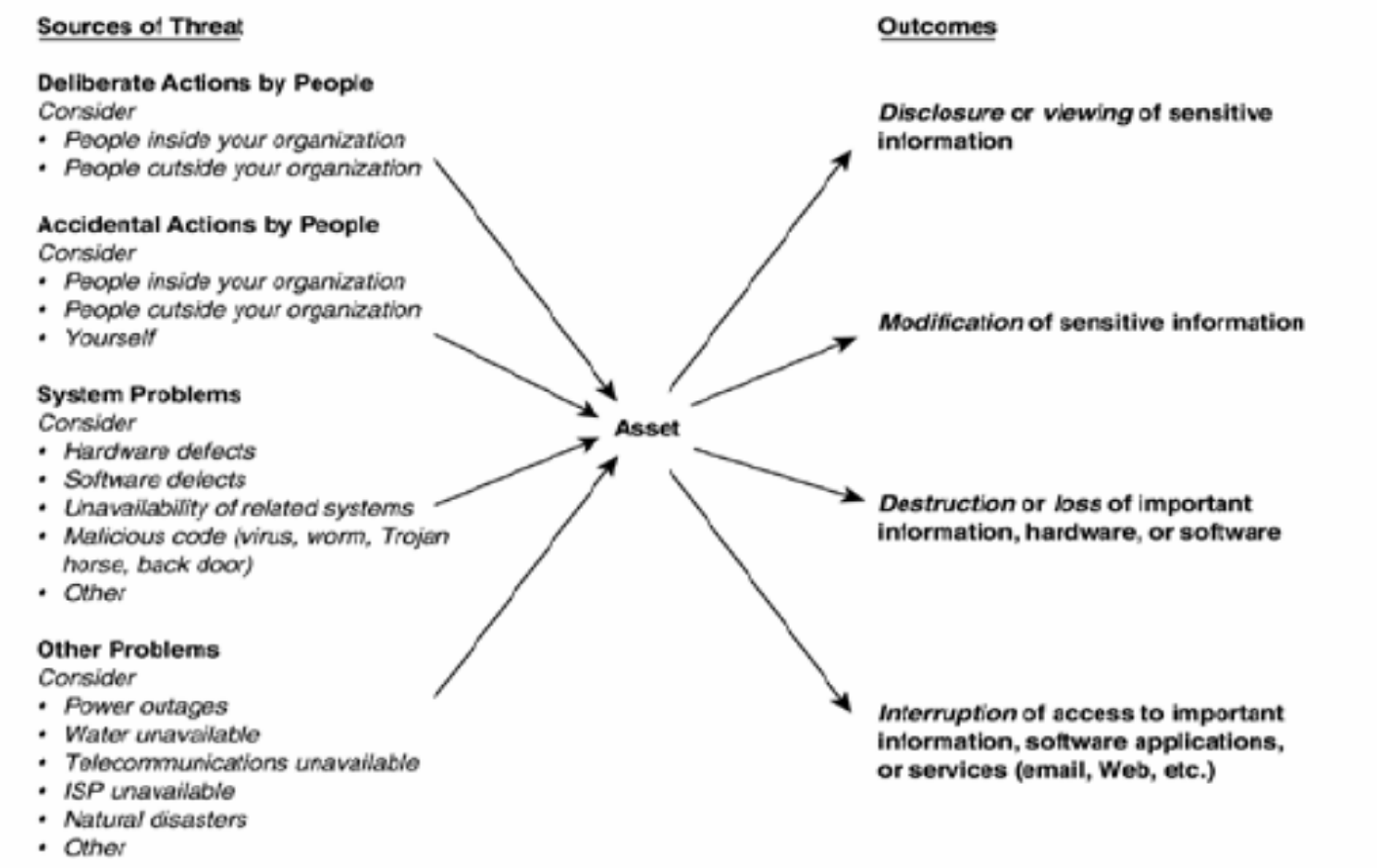
Pada metode OCTAVE, tedapat sumber-sumber ancaman terhadap aset-aset informasi yakni :

a. Tindakan sengaja oleh manusia (***Deliberate Action by People***) baik dari dalam (*inside*) maupun dari luar (*outside*).
b. Tindakan tidak sengaja oleh manusia (***Accidental Action by people***) baik dari dalam (*inside*) maupun dari luar (*outside*).
c. Sistem yang bermasalah (***systems ploblem***) meliputi hardware dan software yang cacat, kode berbahaya (virus worm, trojan, back door).
d. Masalah-masalah lain (***other problems***), seperti padamnya arus listrik, ancaman bencana alam, ancaman lingkungan, gangguan telekomunikasi.

Dari ancaman, memberikan hasil pengaruh (*outcomes*) serangan terhadap aset-aset yakni :

- **Disclosure** → dapat terungkapnya informasi-informasi yang sensitif
- **Modification** → berubahnya informasi yang dilakukan oleh orang yang tidak berhak.
- **Destructive and lost** → kerusakkan dan hilangnya informasi yang sensitif.
- **Interuption** → gangguan akses terhadap informasi yang dibutuhkan.

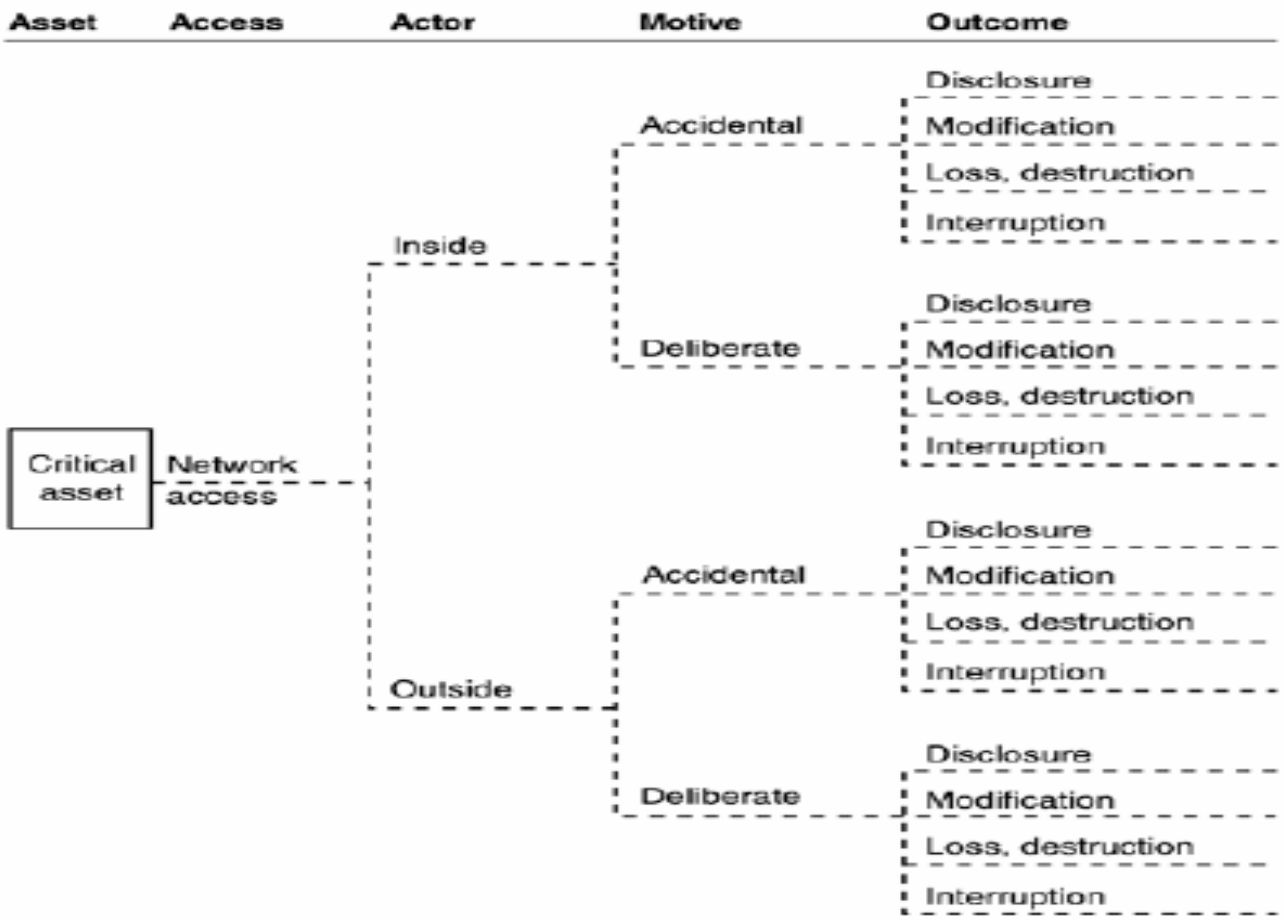
Hal ini tampak pada gambar di bawah berikut →



Gambar 2. Hubungan Sumber Ancaman dan Pengaruhnya terhadap Aset

Dari kondisi diatas, metode OCTAVE didiskripsikan dalam bentuk diagram pohon seperti di bawah ini (**Gambar 3**), untuk memudahkan pemetaan sumber ancaman dan pengaruhnya.

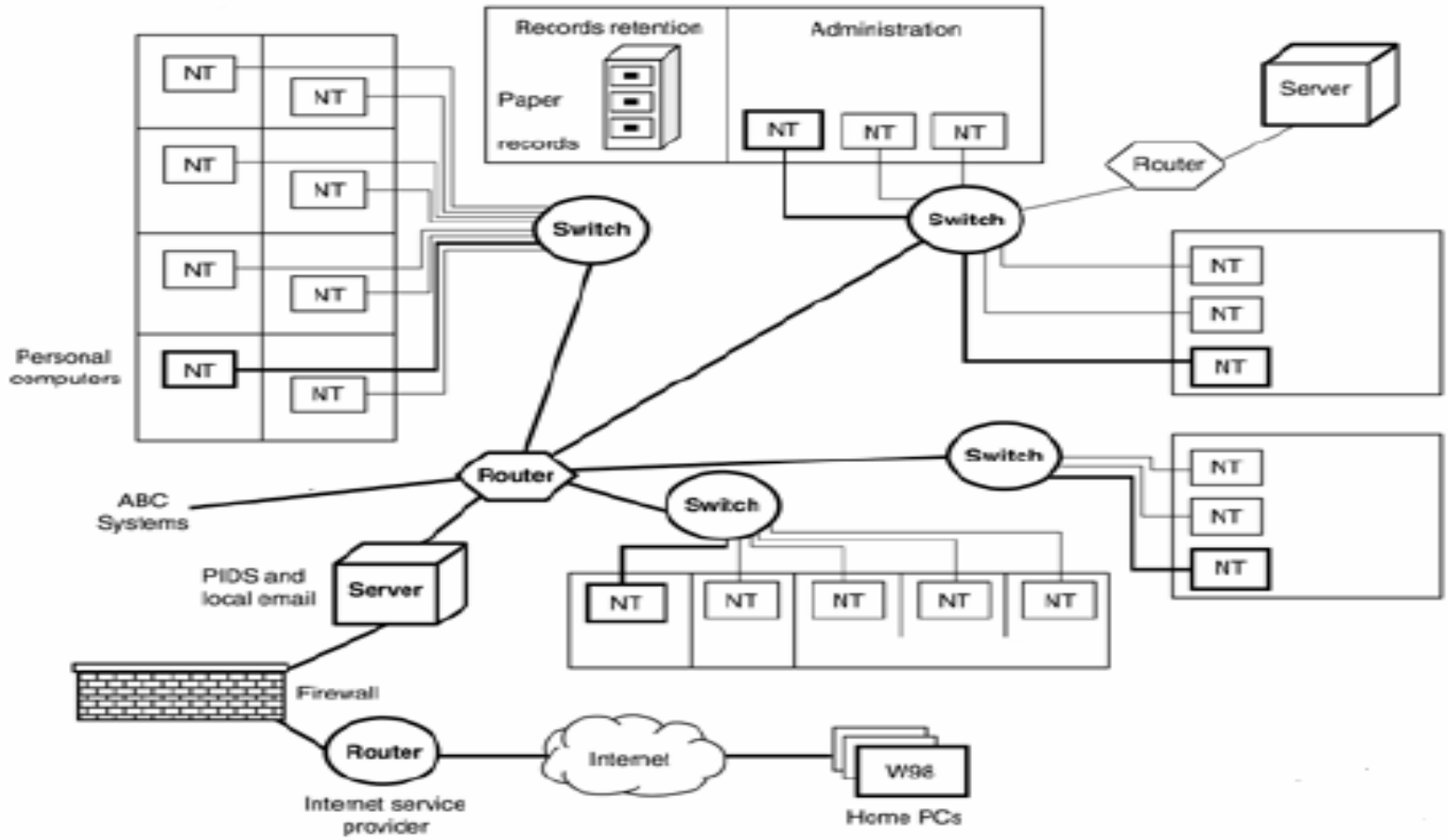
Dimana properti ancaman terdiri dari **aset**, **akses** (cara memperoleh informasi), **aktor** (pelaku yang berasal dari dalam dan luar), **motif** (alasan mengakses informasi sengaja atau tidak disengaja) dan **outcome** (pengungkapan informasi, perubahan, perusakan dan penghilangan serta gangguan akses informasi).



Gambar 3. Diagram Pohon Profil Ancaman

2. **Tahap 2 :** Identifikasi Infrastruktur Vulnerabilities

Tahap kedua melakukan evaluasi kelemahan (***vulnerability***) terhadap jaringan infrastruktur komputasi yang digunakan oleh organisasi. Dilakukan dengan cara menyeleksi komponen-komponen penting yang dapat mempengaruhi kinerja jaringan sistem komputer.



Gambar 4. Komponen Kunci Jaringan Infrastruktur Sistem Informasi

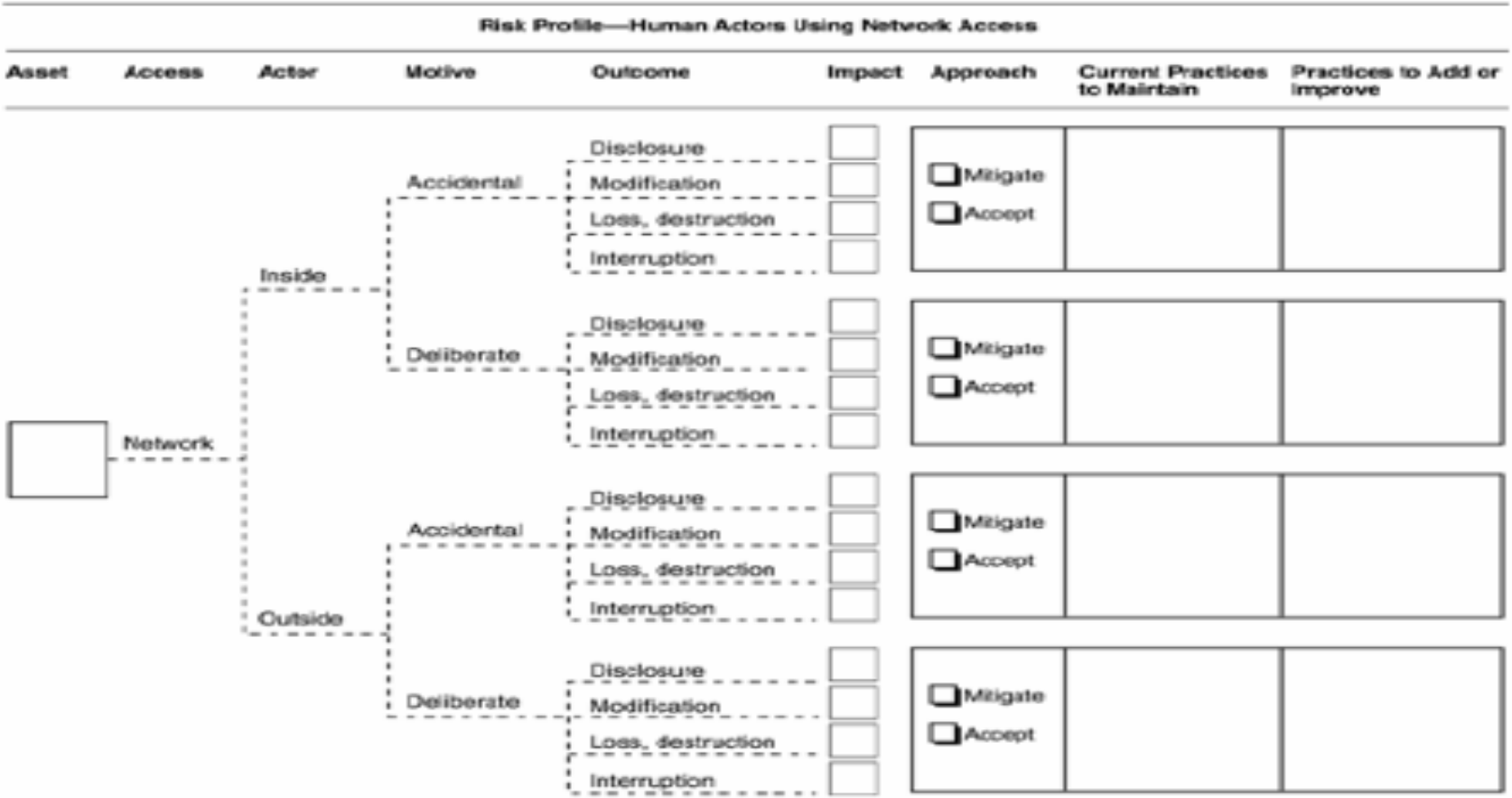
Dari setiap komponen kunci diuji dengan tools/utilitas evaluasi kelemahan (Nmap, Nexsus, dll) baik secara hardware dan software. Kegiatan ini dilakukan untuk mengaudit kelemahan keamanan jaringan dan upaya-upaya penanggulangannya. Pada tahap ini banyak melibatkan staf TI organisasi.

3. **Tahap 3 :** Mengembangkan Strategi Keamanan dan Perencanaannya

Dari tahap I dan II diperoleh profil ancaman dan kelemahan infrastruktur sistem jaringan informasi. Pada tahap III ditindaklanjuti dengan merangkum kegiatan sebelumnya menjadi bentuk profil risiko dengan tingkat ukuran risiko (secara kualitatif) yang dikaitkan dengan dampaknya bagi perusahaan serta rencana mitigasi risiko.

Pada level pengukuran resiko ditentukan secara subyektifitas asumsi yang dimilki organisasi terhadap level risiko.

Profil risiko dideskripsikan dengan diagram pohon seperti berikut ini:



Gambar 5. Profil risiko terhadap ancaman tindakan manusia yang menggunakan akses jaringan

Dampak (***impact***) meliputi dampak reputasi, produktifitas, kostumer, hukum dan keuangan dengan tingkat risko (Rendah (L), sedang (M) dan tinggi (H)) yang kita definisikan secara kualitatif seperti di bawah ini:

Impact				
Reputation	Customer	Productivity	Legal	Financial
L	M	L	L	M
L	L	L	M	M
L	L	L	M	L

Dari hal tersebut kemudian ditentukan rencana untuk mitigasi risiko terkait dengan tingkat risiko yang dimiliki organisasi.

Perbedaan OCTAVE - OCTAVE/S – OCTAVE Alegro

Octave

Pendekatan OCTAVE didefinisikan oleh panduan untuk penerapan metode (prosedur, bimbingan, lembar kerja, katalog informasi) dan pelatihan. Metode ini dilakukan dalam serangkaian *workshop* yang dilakukan dan difasilitasi oleh tim analisis interdisipliner yang diambil dari unit-unit bisnis di seluruh organisasi (misalnya Eksekutif, manajer, pusat operasi dan staf) dan anggota dari departemen TI.

Metode ini juga dirancang untuk memungkinkan menyesuaikan organisasi mengadopsinya. Kebanyakan organisasi yang telah memanfaatkan metode OCTAVE untuk menyesuaikan pendekatan sesuai dengan proses bisnis mereka.

Perbedaan OCTAVE - OCTAVE/S – OCTAVE Alegro

Metode OCTAVE dilakukan dalam tiga tahap. **Pada tahap 1**, tim analisis mengidentifikasi informasi penting yang berkaitan dengan aset dan strategi perlindungan saat ini untuk aset ini. Tim kemudian menentukan yang mana dari aset diidentifikasi yang paling penting bagi keberhasilan organisasi, dokumen persyaratan keamanan mereka, dan mengidentifikasi ancaman yang dapat mengganggu memenuhi persyaratan. **Pada tahap 2**, tim analisis untuk mengevaluasi infrastruktur informasi untuk melengkapi analisis ancaman yang dilakukan pada fase 1 dan untuk menginformasikan keputusan mitigasi dalam tahap 3. Akhirnya, dalam **tahap 3**, tim melakukan identifikasi analisis risiko dan mengembangkan rencana mitigasi risiko untuk aset kritis.

Octave - S

Pengembangan OCTAVE-S didukung oleh *Technology Insertion*, *Demonstration*, dan *Evaluation* (TIDE) program di SEI (Software Engineering Institute), dengan tujuan membawa pendekatan OCTAVE organisasi berbasis manufaktur kecil. Versi terbaru dari pendekatan OCTAVE-S, versi 1.0, secara khusus dirancang untuk organisasi dari sekitar 100 orang atau kurang. Konsisten dengan kriteria OCTAVE, pendekatan OCTAVE-S terdiri dari tiga fase yang sama. Namun, OCTAVE-S dilakukan oleh tim analisis yang memiliki pengetahuan luas tentang organisasi. Jadi, OCTAVE-S tidak tergantung pada lokakarya elisitasi pengetahuan formal untuk mengumpulkan informasi karena diasumsikan bahwa tim analisis (biasanya terdiri dari 3-5 orang) telah bekerja.

Perbedaan lain yang signifikan dalam OCTAVE-S adalah lebih terstruktur daripada metode OCTAVE. Konsep keamanan OCTAVE-S tertanam dalam *worksheet* dan *guidance*, sehingga risiko kurang berpengalaman untuk mengatasi berbagai risiko menjadi lebih kecil. Sebuah fitur yang membedakan dari OCTAVE-S adalah bahwa OCTAVE-S memerlukan pemeriksaan infrastruktur informasi organisasi. Karena organisasi yang lebih kecil mungkin tidak memiliki sumber daya untuk mendapatkan dan menjalankan alat *vulnerability*, OCTAVE-S dirancang untuk pemeriksaan terbatas risiko infrastruktur.

Octave - Allegro

Pendekatan yang diperkenalkan OCTAVE Allegro dalam laporan teknis yang dirancang untuk memungkinkan penilaian keseluruhan lingkungan risiko operasional organisasi untuk menghasilkan hasil yang lebih kuat tanpa memerlukan pengetahuan tentang penilaian risiko. Pendekatan ini berbeda dari sebelumnya, pendekatan OCTAVE berfokus terutama pada informasi dalam konteks bagaimana mereka digunakan di mana mereka disimpan, diangkut dan diproses, dan bagaimana mereka terkena ancaman, kerentanan dan gangguan sesuai. Seperti metode sebelumnya, Allegro OCTAVE bisa dilakukan dalam pengaturan *workshop-style*, kolaboratif dan didukung dengan *guidance*, *worksheet* dan kuesioner. Namun, OCTAVE-Allegro ini juga cocok untuk digunakan oleh orang-orang yang ingin melakukan penilaian risiko tanpa keahlian yang luas.

Pendekatan OCTAVE-Allegro terdiri dari delapan langkah yang ditetapkan dalam empat tahap. Pada tahap 1, organisasi mengembangkan kriteria pengukuran risiko yang konsisten dengan driver organisasi. Tahap kedua, aset informasi yang penting diprofilkan. Proses ini menetapkan batas yang jelas untuk profil aset, mengidentifikasi persyaratan keamanan, dan mengidentifikasi semua lokasi di mana aset disimpan, diangkut, atau diproses. Pada fase 3, ancaman terhadap aset informasi yang diidentifikasi dalam konteks lokasi di mana aset tersebut disimpan, diangkut, atau diproses. Pada tahap akhir, risiko terhadap aset informasi diidentifikasi dan dianalisis dan pengembangan pendekatan mitigasi dimulai.

Thank You !