MANAJEMEN RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION)

Bambang Supradono[1)]
[1)]Jurusan Teknik Elektro Fakultas Teknik
Universitas Muhammadiyah Semarang
Jl. Kasipah no 10 – 12, Semarang – Indonesia
e-mail : bsupradono@gmail.com

ABSTRAK

Untuk mencapai tujuan bisnisnya, seringkali perusahaan atau organisasi menggunakan Teknologi Informasi (TI) dalam mengelola informasi sebagai basis dalam penciptaan layanan yang berkualitas ataupun dalam optimalisasi proses bisnisnya. Meningkatnya tingkat ketergantungan organisasi pada sistem informasi sejalan dengan resiko yang mungkin timbul.

Salah satu risiko yang timbul adalah risiko keamanan informasi, dimana informasi menjadi suatu yang penting yang harus tetap tersedia dan dapat digunakan, serta terjaga keberadaannya dari pihak yang tidak berwenang yang akan menggunakannya untuk kepentingan tertentu atau akan merusak informasi tersebut. Informasi merupakan sebuah aset penting bagi organisasi yang perlu dilindungi dan diamankan.

Kata kunci : teknologi informasi, aset, risiko

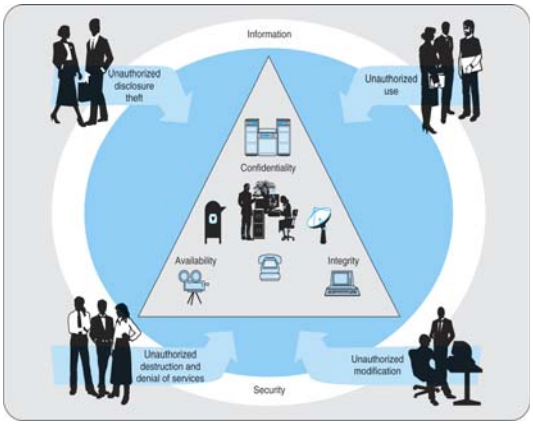
1. Pendahuluan

Aset informasi (hardware, software, sistem, informasi dan manusia) merupakan aset yang penting bagi suatu organisasi yang perlu dilindungi dari risiko keamanannya baik dari pihak luar dan dalam organisasi. Keamanan informasi tidak bisa hanya disandarkan pada tools atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan secara tepat solusi yang dapat menangani permasalahan kebutuhan keamanan informasi). Untuk itu butuh pengelolaan keamanan informasi yang sistemik dan komprehensif. Aspek kebutuhan keamanan informasi harus memuat 3 unsur penting yakni :

1. *Confidentiality (kerahasiaan)* aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity (integritas)* aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), harus terjaga keakuratan dan keutuhan informasi serta
3. *Availability (ketersediaan)* aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait bilamana diperlukan.

Tiga aspek keamanan rawan terhadap ancaman serangan-serangan yang mengancam keberadaanya baik serangan terhadap sumber-sumber informasi baik secara fisik dan melalui akses secara jaringan.

Untuk mengatasi risiko keamanan butuh kemampuan dalam pengelolaan/manajemen risiko keamanan informasi untuk itu dibutuhkan pendekatan ilmu manajemen.



Gambar 1 Tiga unsur aspek keamanan informasi.

2. Framework Manajemen Keamanan Risiko Sistem Informasi

Evaluasi kegiatan mempertimbangkan apa yang terjadi selama evaluasi, ketika sebuah organisasi yang melakukan evaluasi risiko keamanan informasi, maka untuk melakukan kegiatan :

a) Identifikasi
Mengidentifikasi risiko keamanan informasi (merekam profil risiko dan informasi organisasi)

b) Analisis
Menganalisis risiko untuk menvaluasi risiko dan menentukan prioritas

c) Plan

Rencana untuk perbaikan perlindungan oleh mengembangkan strategi untuk perbaikan organisasi dan rencana mitigasi risiko untuk mengurangi risiko untuk aset penting organisasi

Evaluasi hanya menyediakan arah organisasi sebuah kegiatan keamanan informasi; tidak selalu berarti mengarah ke perbaikan.. Setelah evaluasi, organisasi harus mengambil langkah-langkah berikut:

d) Plan

Merencanakan cara untuk menerapkan strategi perlindungan dan mitigasi risiko dari rencana pengembangan rinci oleh evaluasi rencana aksi. Kegiatan ini dapat mencakup rinci analisis biaya-manfaat antara strategi dan tindakan.

e) Implementasi

Melaksanakan rencana aksi dipilih secara rinci.

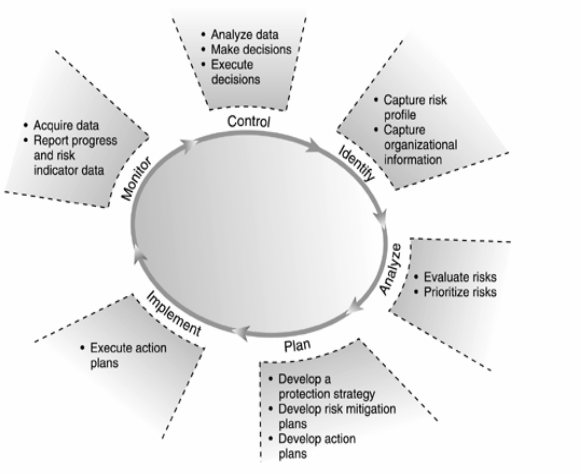
f) Monitor

Memantau kemajuan dan efektifitas, kegiatan ini meliputi pemantauan risiko untuk setiap perubahan.

g) Control

Mengontrol pelaksanaanya telah sesuai dengan tindakan korektif, dengan cara menganalsis data, membuat keptusan dan meneksekusi hasil keputusan yang dibuat.

Siklus ini dikerjakan secara berkesinambungan berkaiatan dengan peningkatan dan penambahan risiko yang selalu muncul mengancam keamanan informasi. General Accounting Office (GAO) membuat pedoman dalam mengelola risiko seperti gambar di bawah ini :



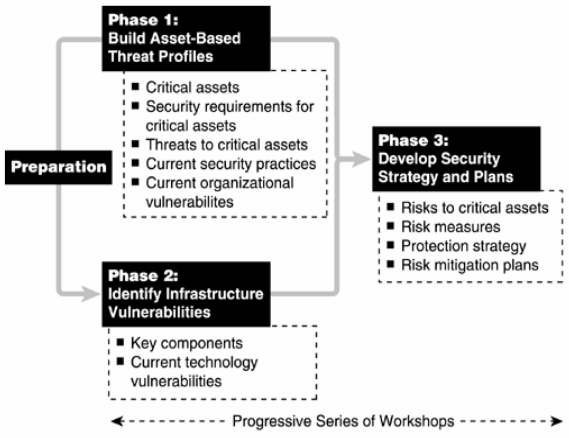
Gambar 2 Siklus Framework berdasar GAO, 98

3. Metode OCTAVE

Untuk mengelola risiko keamanan informasi adalah mengenali apakah risiko organisasi yang menerapkannya. Setelah risiko diidentifikasi, organisasi dapat membuat rencana penanggulangan dan mengurangi/mitigasi risiko terhadap masing-masing risiko yang telah diketahui. Metode OCTAVE (*The Operationally Critical Threat, Asset, and Vulnerability Evaluation)* yang dikembangkan Software Engineering Institute, Carnegie Mellon University, 1999 memungkinkan organisasi melakukan hal di atas.

OCTAVE 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. Pada akhirnya, 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 3 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 adalah :

a) Tahap Persiapan :

Pada tahap ini adalah kegiatan persiapan yang harus dilkasanakan sebelum melaksanakan metode OCTAVE yakni :

menyusun jadwal, membentuk tim analisis, meminta dukungan dan menyiapkan logistik.

b) Tahap 1: Membangun Aset Berbasis Ancaman Profil

Keluaran dalam tahap 1 ini meliputi

i. Aset-aset yang penting bagi organisasi
ii. Kebutuhan keamanan aset-aset penting yang tidak terlepas dari 3 aspek keamanan yaknik kerahasiaan, integritas dan ketersediaaan.
iii. Praktek-praktek keamanan terkini yang dimiliki organisasi atau upaya organisasi untuk melindungi aset informasi
iv. Kelemahan kebijakkan organisasi terkini.

c) Tahap 2: Identifikasi Infrastruktur Vulnerabilities

Ini adalah evaluasi informasi infrastruktur jaringan komputer. Komponen operasional kunci dari infrastruktur teknologi informasi (server, PC, laptop dan perangkat jaringan) diidentifikasi kelemahannya baik dari sisi teknologi dan konfigurasi, yang dapat menimbulkan akses keamanan oleh yang tidak berhak menjadi mudah

d) Tahap 3: Mengembangkan Strategi Keamanan dan Perencanaannya

Keluaran dari tahapan ini adalah :

i. Risiko-risiko terhadap aset-aset penting
ii. Mengukur tingkat risiko
iii. Strategi proteksi
iv. Rencana-rencana pengurangan/mitigasi risiko

4. Analisa dan Pembahasan

4.1. Tahap I Membangun Aset Berbasis Ancaman Profil

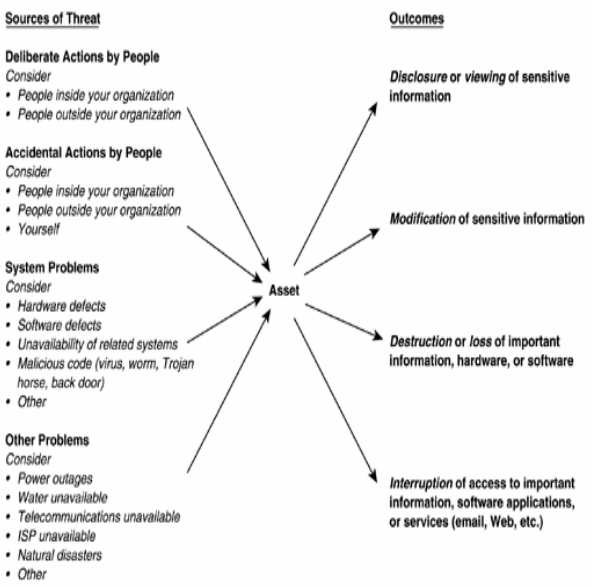
Pada metode OCTAVE sumber-sumber ancaman terhadap aset-aset indormasi dalam 4 sumber yakni :

i. Tidakan sengaja oleh manusia *(Deliberate Action by People)* baik dari dalam (*inside*) maupun dari luar (*outside*).
ii. Tindakan tidak sengaja oleh manusia *(Accidental Action by people)* baik dari dalam (*inside*) maupun dari luar (*outside*).
iii. Sistem yang bermasalah (*systems ploblem*) meliputi hardware dan software yang cacat, kode berbahaya (*virus worm, trojan, back door).*
iv. 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.

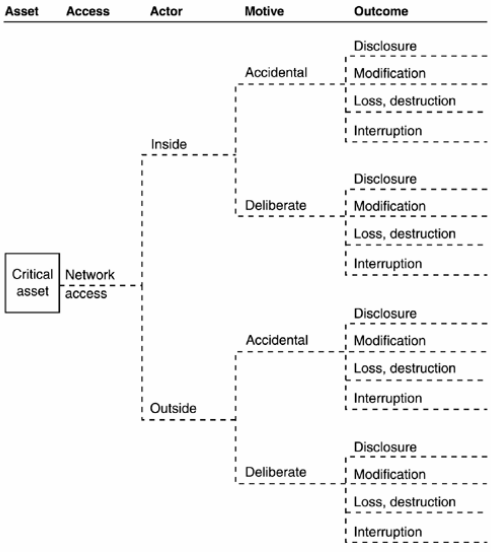
Hal ini nampak pada gambar di bawah ini :



Gambar 4 Hubungan sumber ancaman dan pengaruhnya terhadap aset.

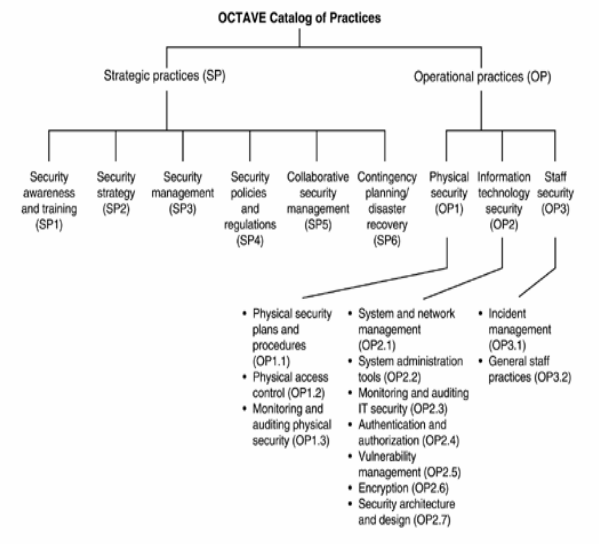
Dari kondisi diatas metode OCTAVE mendiskripsikan dalam bentuk diagram pohon seperti di bawah ini untuk memudahkan pemetaan sumber ancaman dan pengaruhnya.

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, perusakkan dan penghilangan serta gangguan akses informasi).



Gambar 5 Diagram pohon profil ancaman.

Kemudian dilanjutkan dengan mengevaluasi katalog-katalog praktek-praktek keamanan.

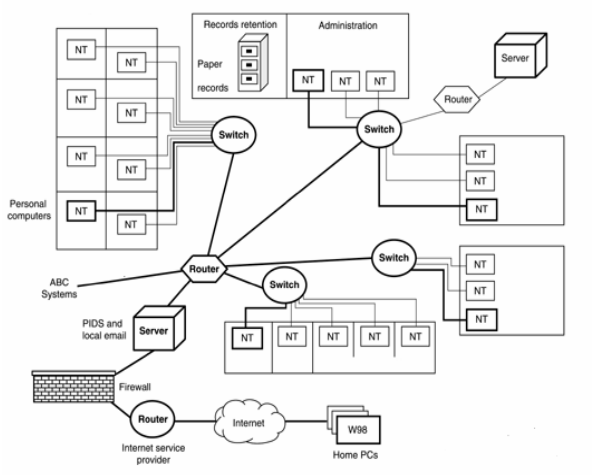


Gambar 6 Diagram dokumentasi katalog dan praktek-praktek metode OCTAVE.

Apabila terdapat dokumen-dokumen yang tesebut pada gambar di atas maka bisa dilakukan uji kepatuhan (*compliance test*). Jika tidak ada dokumen maka diupayakan untuk membuat dokumen iuntuk memudahkan evaluasi.

4.2. Tahap II Identifikasi Infrastruktur Vulnerabilities

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



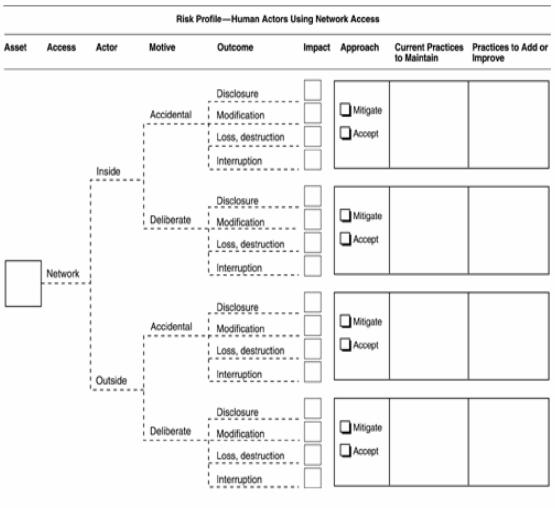
Gambar 7 Komponen kunci jaringan infrastruktur sistem informasi

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.

4.3. Tahap III 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 8. Profil risiko terhadap ancaman tindakan manusia yang menggunakan akses jaringan.

Dampak *(impact)* meliputi dampak reputasi, produktifitas, kostumer, hukum dan keuangan dengan tingkat risko (Rendah, sedang dan tinggi) 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.

5. Kesimpulan

Metode OCTAVE memberikan panduan secara sistemik dan komprehensif dalam manajemen risiko keamanan informasi. Metode ini lebih menekankan pengelolaan risiko berbasis ancaman *(threat)* dan kelemahan *(vulnerability)* terhadap aset-aset informasi organisasi meliputi perangkat keras, lunak, sistem, informasi dan manusia.

6. Daftar Pustaka

1. Alberts, Christopher and Dorofee, Audrey, *Managing Information Security Risks: The OCTAVE^{SM} Approach*, 2002.
2. Alberts, Christopher and Dorofee, Audrey. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE^{SM}) Criteria (CMU/SEI-01-TR-016). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. Available online: <http://www.sei.cmu.edu/publications/documents/01.reports/01tr016/01tr016abstract.html >.
3. United States General Accounting Office. Executive Guide: Information Security Management (GAO/AIMD-98-68). Washington, DC: GAO, 1998