

## PERBANDINGAN METODOLOGI EVALUASI RISIKO KEAMANAN INFORMASI OCTAVE-S DAN OCTAVE ALLEGRO

**Humaira**

Teknologi Informasi, Politeknik Negeri Padang, Padang  
Email: [mira.humaira@gmail.com](mailto:mira.humaira@gmail.com)

**Abstrak** - Keamanan Informasi menjadi hal krusial dalam sebuah perusahaan. Menurut survey CyberSecurity Watch yang dilakukan tahun 2011 bahwa serangan yang dilakukan orang dalam (pegawai perusahaan) memberikan dampak kerusakan yang parah dibandingkan serangan dari luar. Oleh karena itu perusahaan perlu melakukan evaluasi terhadap kemungkinan risiko informasi yang dimilikinya. Makalah ini membahas dua metode evaluasi risiko keamanan informasi yaitu OCTAVE-S dan OCTAVE Allegro. Metode OCTAVE – S dipersiapkan untuk organisasi kecil dimana melakukan evaluasi terhadap kemungkinan risiko kemudian membuat perencanaan strategis. Sedangkan OCTAVE Allegro melakukan evaluasi secara rinci terhadap risiko kemudian memberikan penilaian risiko.

**Kata Kunci** : Keamanan Informasi OCTAVE-S, OCTAVE Allegro

### 1. PENDAHULUAN

Pemanfaatan Teknologi Informasi (TI) dalam suatu perusahaan, dalam implementasinya selain didapatkan manfaat dari TI tentu akan diimbangi dengan berbagai risiko teknologi informasi yang dapat mempengaruhi pencapaian sasaran perusahaan. Mengingat bahwa TI merupakan aset penting maka harus dikelola secara efektif guna memaksimalkan efektifitas penggunaannya dan agar risiko terkait dari teknologi yang diimplementasikan dapat dimitigasi.

Menurut laporan survey *cyber Security Watch* bahwa tahun 2011 bulan Januari ditemukan serangan sebesar 58% yang disebabkan oleh orang luar (tidak memiliki kewenangan untuk akses ke sistem jaringan maupun data) sebaliknya 21% dari serangan disebabkan oleh orang dalam (karyawan atau kontraktor yang memiliki akses) resmi dan 21% tidak dikenal [HYPERLINK \l "2011" 1].

Salah satu risiko TI yaitu masalah keamanan data. Data perusahaan dan pelanggan sangat penting untuk kesuksesan bisnis. Dalam dunia TI sekarang ini sering terjadi pencurian identitas dan pencurian data, banyak perusahaan kecil tidak siap untuk menangani beban tanggung jawab terhadap data yang dimiliki.

Mengamankan data berarti memahami potongan informasi yang perlu dilindungi dan memberlakukan prosedur yang tepat dan perlindungan untuk menjaga informasi ini supaya aman. Beberapa jenis informasi dengan prioritas tinggi yang perlu diamankan2]:

#### 1. Informasi Pelanggan

Pengamanan data pelanggan harus menjadi prioritas nomor satu untuk setiap bisnis. Tanpa pelanggan, bisnis ini akan

gagal. Dan tanpa keamanan data, pelanggan akan membawa bisnis mereka ke perusahaan pesaing. Dalam perekonomian saat ini di seluruh dunia, pelanggan memiliki banyak pilihan. Mengamankan data pelanggan membuat pelanggan senang.

#### 2. Informasi Produk

Dalam banyak industri, melindungi informasi tentang produk baru dan yang sudah ada juga menjadi prioritas. Inovasi adalah kunci untuk bertahan dalam kebanyakan bisnis, dan dalam rangka untuk melindungi kekayaan intelektualnya, perusahaan harus memperhatikan keamanan data ini.

#### 3. Informasi Karyawan

Sebagian besar perusahaan memiliki detail informasi pribadi tentang karyawan, seperti nomor jaminan sosial, alamat, nomor telepon, dan catatan kerja. Ini penting untuk keberhasilan sebuah bisnis untuk melindungi kepentingan karyawan. Karyawan merupakan aset bagi perusahaan.

#### 4. Informasi Perusahaan

Hal ini penting bagi banyak perusahaan untuk melindungi informasi keuangan dan data lain tentang bisnis. Jika diakses oleh pengguna yang tidak sah, informasi ini dapat membahayakan reputasi bisnis atau memberikan dorongan bagi tindakan hukum terhadap perusahaan. Melindungi informasi perusahaan sangat penting.

Saat ini belum ada manajemen risiko yang khusus menangani bidang Teknologi Informasi. Dari paparan diatas, bidang TI banyak menimbulkan berbagai macam ancaman internal maupun

eksternal serta kelemahan dari segi teknologi yang akan merongrong organisasi.

Oleh karena itu makalah ini akan mempelajari dan menganalisa pendekatan metodologi evaluasi risiko keamanan informasi yang dikenal dengan OCTAVE. Sehingga organisasi dapat memilih jenis metodologi yang cocok di lingkungan organisasinya.

## 2. MANAJEMEN RESIKO TI

Setiap organisasi memiliki misi. Dalam era digital, sebagai organisasi menggunakan sistem Teknologi Informasi untuk memproses informasi yang lebih baik. Risiko manajemen memainkan peran penting dalam melindungi aset informasi organisasi. Suatu proses manajemen risiko yang efektif merupakan komponen penting dari keberhasilan keamanan program TI. Tujuan utama dari proses manajemen risiko untuk melindungi organisasi dan kemampuannya dalam melakukan misi, bukan hanya aset TI. Oleh karena itu, manajemen risiko tidak harus ditangani oleh fungsi teknis TI yang mengoperasikan dan mengelola sistem TI, tetapi merupakan suatu fungsi manajemen yang penting dari organisasi.

Risiko adalah sesuatu hal tidak pasti yang berdampak negatif dari kejadian. Manajemen risiko adalah proses identifikasi risiko, penilaian risiko, dan mengambil langkah-langkah untuk mengurangi risiko ketinggian yang dapat diterima. Panduan ini memberikan landasan bagi pengembangan program manajemen risiko yang efektif, yang mengandung definisi dan diperlukan untuk menilai dan mengurangi risiko yang teridentifikasi dalam sistem TI. Tujuan utamanya adalah untuk membantu organisasi untuk lebih baik mengelola risiko TI yang berhubungan dengan misi organisasi.

Metode-metode manajemen risiko [HYPERLINK \ "Asi11" 2 ] adalah sebagai berikut:

- **Pengurangan Risiko (Peringatan Risiko)**  
Ini dilakukan ketika kemungkinan ancaman/kerentanan tinggi tetapi dampaknya rendah. Diperlukan pemahaman akan ancaman dan kerentanan yang ada, mengubah atau menguranginya, dan membangun pertahanan. Akan tetapi, pengurangan risiko tidak mengurangi nilai risiko menjadi '0'.
- **Penerimaan Risiko**  
Ini dilakukan ketika kemungkinan ancaman/kerentanan rendah dan dampaknya kecil atau dapat diterima.
- **Pemindahan Risiko**  
Jika risiko sangat tinggi atau organisasi tidak mampu mempersiapkan kendali yang diperlukan, risiko dapat dipindahkan

keluar dari organisasi. Contohnya adalah dengan mengambil polis asuransi.

- **Penghindaran Risiko**

Jika ancaman dan kerentanan sangat mungkin terjadi dan dampaknya juga sangat tinggi, lebih baik menghindari risiko dengan misalnya melakukan alih daya perangkat pemrosesan data dan juga staf.

### Aset Informasi (IAP)

Informasi adalah salah satu aset bagi sebuah perusahaan atau organisasi, yang sebagaimana aset lainnya memiliki nilai tertentu bagi perusahaan atau organisasi tersebut sehingga harus dilindungi, untuk menjamin kelangsungan perusahaan atau organisasi, meminimalisir kerusakan karena kebocoran sistem keamanan informasi, mempercepat kembalinya investasi dan memperluas peluang usaha2]. Beragam bentuk informasi yang mungkin dimiliki oleh sebuah perusahaan atau organisasi meliputi diantaranya: informasi yang tersimpan dalam komputer (baik *desktop* komputer maupun *mobile* komputer), informasi yang ditransmisikan melalui network, informasi yang dicetak pada kertas, dikirim melalui fax, tersimpan dalam disket, CD, DVD, *flashdisk*, atau media penyimpanan lain, informasi yang dilakukan dalam pembicaraan (termasuk percakapan melalui telepon), dikirim melalui telex, email, informasi yang tersimpan dalam basisdata, tersimpan dalam film, dipresentasikan dengan OHP atau media presentasi yang lain, dan metode-metode lain yang dapat digunakan untuk menyampaikan informasi dan ide-ide baru organisasi atau perusahaan .

Tabel 1 Perbandingan Aset Informasi dan Aset Nyata [HYPERLINK \ "Asi11" 2 ]

Karakteristik	Aset informasi	Aset nyata
<b>Bentuk Pemeliharaan</b>	Tidak memiliki bentuk fisik dan bersifat fleksibel	Memiliki bentuk fisik
<b>Variable Nilai</b>	Bernilai lebih tinggi ketika digabung dan diproses	Total nilai adalah jumlah dari tiap nilai
<b>Berbagi</b>	Reproduksi yang tak terbatas dan orang-orang dapat berbagi nilainya	Reproduksi tidak mungkin
<b>Ketergantungan Medium</b>	Perlu disampaikan melalui medium	Dapat disampaikan secara independen(karena bentuk fisiknya)

Seperti yang terlihat pada Tabel 1, aset informasi jelas berbeda dengan aset nyata. Oleh karena itu, aset informasi rentan terhadap berbagai jenis risiko.

**Keamanan Informasi**

Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki. Kebanyakan orang mungkin akan bertanya, mengapa “keamanan informasi” dan bukan “keamanan teknologi informasi” atau *IT Security*. Kedua istilah ini sebenarnya sangat terkait, namun mengacu pada dua hal yang sama sekali berbeda. Keamanan Teknologi Informasi atau *IT Security* mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan. Berbeda dengan keamanan informasi yang fokusnya justru pada data dan informasi milik perusahaan. Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan.

Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut3]:

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 diubah tanpa ada ijin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas ini.
3. *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).
4. *Authentication* (otentikasi) meyakinkan keaslian data, sumber data, orang yang mengakses data dan server yang digunakan.
5. *Non-repudiation* yaitu tidak dapat menyangkal (telah melakukan transaksi)
6. *Access Control* yaitu Mekanisme untuk mengatur siapa boleh melakukan apa

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

**4R keamanan informasi**

4R keamanan informasi adalah *Right Information* (Informasi yang benar), *Right People* (Orang yang

tepat), *Right Time* (Waktu yang tepat) dan *Right Form* (Bentuk yang tepat). Pengaturan 4R adalah cara paling efisien untuk memelihara dan mengontrol nilai informasi [ [HYPERLINK \l "Asi11" 2](#) ].

- Informasi yang benar mengacu pada ketepatan dan kelengkapan informasi, menjamin keutuhan informasi.
- Orang yang tepat berarti informasi tersedia bagi individu yang berhak, sehingga menjamin kerahasiaan.
- Waktu yang tepat mengacu pada kemudahan akses informasi dan penggunaannya atas permintaan entitas yang berhak. Ini menjamin ketersediaan.
- Bentuk yang tepat mengacu pada penyediaan informasi dalam format yang tepat.

4R harus digunakan dengan tepat untuk menjaga keamanan informasi. Ini berarti bahwa kerahasiaan, integritas dan ketersediaan haruslah ditinjau ketika menangani informasi.

**3. OCTAVE**

**Definisi OCTAVE**

OCTAVE ® (*Operational Critics Threat, Asset, and Vulnerability Evaluation*) merupakan pendekatan evaluasi risiko keamanan informasi yang komprehensif, sistematis, *context driven* dan langsung dilakukan sendiri oleh organisasi yang bersangkutan4]. OCTAVE juga dapat dipandang sebagai sebuah *tool* untuk meningkatkan keamanan informasi.

OCTAVE sebagai metodologi pengambilan keputusan yang fokus pada perlindungan sumber daya di dalam sebuah organisasi. Pada juni 1999, SEI (*Software Engineering Institute*) mengeluarkan laporan mengenai framework OCTAVE. Framework ini khusus mengevaluasi risiko keamanan informasi dimana organisasi besar sebagai targetnya [ [HYPERLINK \l "Chr01" 5](#) ].

Saat membangun framework, sasarannya menentukan syarat pendekatan umum sebagai bahan evaluasi dan mengatur risiko keamanan informasi. Pada akhirnya disadari bahwa pendekatan umum yang diimplementasikan pada organisasi kecil dengan 10 karyawan tentunya berbeda dengan corporate multi nasional. Oleh karena itu, perkembangan OCTAVE perlu pendekatan dikedua jenis organisasi besar maupun kecil.

Tabel 2 Perkembangan OCTAVE [ [HYPERLINK \l "Ric07" 6](#) ]

Tanggal	Publikasi
September	OCTAVE Framework version 1.0

<b>1999</b>	
<b>September 2001</b>	OCTAVE Framework version 2.0
<b>Desember 2001</b>	OCTAVE Criteria version 2.0
<b>September 2003</b>	OCTAVE – S v0.9
<b>Maret 2005</b>	OCTAVE – S v1.0
<b>Juni 2007</b>	Memperkenalkan OCTAVE Allegro v1.0

### Struktur Kriteria OCTAVE

Pendekatan OCTAVE didefinisikan dalam sekumpulan kriteria termasuk prinsip, atribut dan output]. Prinsip merupakan konsep dasar evaluasi. Sebagai contoh petunjuk diri sendiri termasuk prinsip dari OCTAVE. Artinya orang yang berada dalam organisasi adalah posisi yang paling baik untuk melakukan evaluasi dan membuat keputusan. Sedangkan atribut turunan dari prinsip OCTAVE. Sebagai contoh salah satu atribut adalah analisis tim oleh personal dalam organisasi tersebut. Terakhir output berupa hasil dari tim analisis yang dicapai selama evaluasi.

Berikut penjelasan masing-masing kriteria [ [HYPERLINK \l "Chr01" 5](#) ]:

#### A. Prinsip OCTAVE

Prinsip adalah konsep dasar proses evaluasi. Prinsip disini di kelompokkan menjadi tiga yaitu:

1. Evaluasi risiko keamanan informasi, merupakan aspek kunci yang membentuk dasar dari evaluasi risiko keamanan informasi yang efektif :
  - Petunjuk dari diri sendiri
  - Ukuran yang sesuai
  - Penentuan proses
  - Dasar untuk proses yang berkesinambungan
2. Manajemen Risiko, merupakan prinsip dasar praktek manajemen risiko yang efektif
  - *Forward-looking*
  - Fokus pada beberapa hal kritis
  - Manajemen terpadu
3. Organisasi dan Budaya, merupakan aspek organisasi dan budaya perusahaan yang penting untuk keberhasilan pengelolaan risiko keamanan informasi
  - Komunikasi terbuka
  - Perspektif global dan kerja sama

#### B. Atribut

Atribut adalah sifat khas, atau karakteristik dari evaluasi. Persyaratan pendekatan OCTAVE dan menentukan apa yang diperlukan untuk membuat evaluasi yang sukses dari proses dan perspektif organisasi. Setiap atribut OCTAVE didefinisikan dengan menggunakan:

- Persyaratan : elemen penting dari atribut
- Kepentingan : mengapa atribut penting untuk proses evaluasi

#### C. Output OCTAVE

Kriteria OCTAVE menentukan pendekatan untuk mengevaluasi risiko keamanan informasi organisasi. Output OCTAVE menentukan hasil bahwa evaluasi tim analisis harus tercapai. Hasilnya evaluasi dibagi sesuai dengan kategori data. Tipe data yang dihasilkan dari proses evaluasi risiko keamanan informasi adalah:

- Data Organisasi
- Data Teknologi
- Analisis risiko serta penanggulangan data

OCTAVE berdasarkan aspek-aspek dasar yang memungkinkan personal organisasi untuk merakit sebuah gambaran yang komprehensif tentang kebutuhan keamanan informasi organisasi. Ada tiga fase metode OCTAVE] yaitu:

1. Tahap1: Membangun Aset Berbasis Ancaman Profil
2. Tahap2: Identifikasi Kerentanan
3. Tahap3: Mengembangkan Strategi dan Rencana Keamanan

#### Metode OCTAVE

Saat ini ketergantungan terhadap data digital yang dapat diakses, dapat diandalkan dan perlindungan dari penyalahgunaan. Sebagian besar organisasi bergantung pada akses data digital untuk melakukan bisnis, data perlu dilindungi dari penyalahgunaan. Kepentingan data yang dapat diakses menjadi ancaman baru bagi organisasi yang dapat berdampak bagi informasi organisasi tersebut.

Kemampuan organisasi untuk mencapai misi dan tujuan bisnisnya secara langsung terkait dengan keadaan infrastruktur komputasi dan cara di mana orang berinteraksi. Bagi suatu organisasi mencapai misinya, orang-orangnya perlu memahami aset informasi yang penting, serta apa yang mereka harus lakukan untuk melindungi aset tersebut. Dengan kata lain, orang-orang dalam organisasi perlu terlibat dalam evaluasi.

Pendekatan OCTAVE membuat organisasi memahami dan memberikan perhatian khusus mengenai risiko keamanan informasi Metode ini fokus pada aset dan risiko terhadap aset. Unsur penting pendekatan OCTAVE terdapat pada sekumpulan kriteria. Organisasi dapat mengembangkan metode yang sesuai dengan kriteria.

OCTAVE adalah evaluasi secara mandiri mengenai risiko keamanan informasi. Konsep inti OCTAVE didefinisikan sebagai suatu situasi di mana orang dari organisasi mengelola dan mengarahkan evaluasi risiko keamanan informasi bagi organisasi mereka. Dalam OCTAVE, tim terdiri dari berbagai

disiplin ilmu yang disebut sebagai tim analisis [HYPERLINK \l "Chr05" 7].

Risiko adalah kemungkinan menderita kerusakan atau kerugian. Tiga komponen dasar risiko: aset, ancaman, dan kerentanan[8]. OCTAVE merupakan pendekatan evaluasi *aset-driven*. Hal ini membutuhkan suatu analisis tim:

- mengidentifikasi aset informasi yang berhubungan (misalnya, informasi dan sistem) yang penting bagi organisasi
- Fokus kegiatan analisis risiko atas aset yang dinilai paling penting untuk organisasi

Ketika tim OCTAVE selesai, ini akan menciptakan strategi perlindungan bagi organisasi dengan perbaikan dan mengurangi risiko terhadap aset kritis organisasi. Dengan demikian, OCTAVE menggabungkan kedua pandangan strategis dan taktis risiko.

Ada tiga metode OCTAVE [ HYPERLINK \l "Car11" 4 ]:

- OCTAVE asli, yang membentuk dasar bagi tubuh OCTAVE pengetahuan
- OCTAVE-S, untuk organisasi yang lebih kecil
- OCTAVE-Allegro, suatu pendekatan yang efisien untuk penilaian dan kepastian keamanan informasi

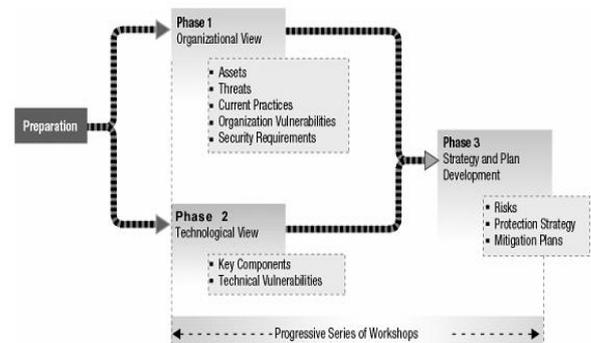
Metode OCTAVE berdasarkan pada pendekatan-OCTAVE kriteria standar untuk melakukan evaluasi terhadap risiko informasi. Kriteria OCTAVE menetapkan prinsip-prinsip dasar dan atribut manajemen risiko yang digunakan oleh metode OCTAVE.

Metode OCTAVE adalah tim yang ditunjuk sendiri oleh personil organisasi di seluruh unit bisnis dan teknologi informasi bekerja sama untuk menangani kebutuhan keamanan organisasi. Setiap metode bersifat fleksibel dimana dapat disesuaikan dengan risiko keamanan yang unik bagi organisasi, memiliki tujuan keamanan, dan tingkat keterampilan. Evolusi OCTAVE memindahkan organisasi terhadap pandangan berbasis risiko dalam konteks bisnis[5].

#### 4. PEMBAHASAN

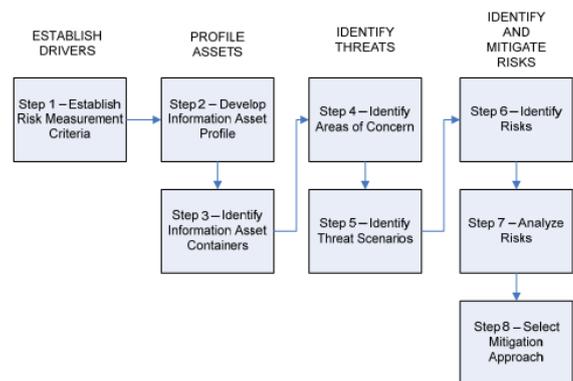
OCTAVE – S dikembangkan untuk memenuhi kebutuhan organisasi kecil. Pada dasarnya, metode OCTAVE dan OCTAVE – S memiliki basis yang sama. OCTAVE-S adalah variasi dari pendekatan yang disesuaikan dengan keterbatasan sarana dan kendala yang unik biasanya ditemukan dalam organisasi kecil (kurang dari 100 orang). OCTAVE-S dipimpin oleh sebuah tim kecil yang berjumlah tiga sampai lima orang dari berbagai disiplin ilmu. Anggota tim mengumpulkan dan

menganalisa informasi kemudian menghasilkan strategi perlindungan dan membuat rencana berdasarkan risiko yang unik dalam keamanan operasional organisasi. Untuk melakukan OCTAVE-S secara efektif, tim harus memiliki pengetahuan yang luas tentang bisnis organisasi dan proses keamanan, sehingga akan dapat melakukan semua kegiatan dengan sendirinya.



Gambar 1 Tahapan metode OCTAVE [ HYPERLINK \l "Chr01" 5 ]

OCTAVE Allegro adalah metodologi untuk merampingkan dan mengoptimalkan proses penilaian risiko keamanan informasi sehingga organisasi dapat memperoleh hasil yang cukup dengan investasi kecil dalam waktu, orang, dan sumber daya terbatas lainnya[6]. Ini akan mengarahkan organisasi untuk mempertimbangkan orang, teknologi, dan fasilitas dalam konteks hubungan informasi dan proses bisnis serta layanan yang didukung.



Gambar 2 Roadmap OCTAVE Allegro [ HYPERLINK \l "Ric07" 6 ]

OCTAVE-S maupun OCTAVE Allegro menggunakan prinsip OCTAVE yaitu tim analisis merupakan pegawai organisasi yang bersangkutan. Dari laporan *CyberSecurity Watch* tahun 2011[1] bahwasanya dari 46% responden menyatakan kerusakan yang disebabkan oleh serangan dari dalam lebih parah dari pada serangan luar. Oleh karena itu keterlibatan orang dalam dalam evaluasi ini sangat berperan penting.

Dari tahun kemunculannya OCTAVE-S lebih dulu di publish daripada OCTAVE Allegro. Sasaran OCTAVE – S ini untuk organisasi kecil. Dilihat dari roadmap OCTAVE-S ini lebih sedikit dan lebih mudah dilakukannya analisis.

Setelah dilakukan penjabaran mengenai OCTAVE – S dan OCTAVE Allegro didapatkan sebuah pemahaman bahwa OCTAVE Allegro dalam mengidentifikasi kelemahan dan ancaman di suatu organisasi disertakan penilaian kualitatif terhadap risiko yang ditimbulkan. Nilai ini akan berdampak terhadap pendekatan investasi organisasi terhadap manajemen risiko TI bisa diukur.

Tabel 3 Perbandingan metode OCTAVE

Atribut	OCTAVE – S	OCTAVE Allegro
<b>Tahun kemunculan</b>	2003	2007
<b>Jenis Organisasi</b>	Kecil	Sedang – Besar
<b>Tingkat Fase</b>	Tiga	Delapan
<b>Menilai risiko</b>	Tidak	Ya

## 5. KESIMPULAN

- a) OCTAVE merupakan salah satu pendekatan metodologi evaluasi risiko keamanan informasi yang dikeluarkan oleh CERT.
- b) Salah satu prinsip dari kriteria OCTAVE yaitu analisis dilakukan oleh tim dari organisasi itu sendiri. Ini sangat menguntungkan bagi organisasi dimana orang dalam organisasi lebih memahami pentingnya informasi bagi kelangsungan bisnis dan menjaga kerahasiaan data organisasi dari pihak ketiga.
- c) OCTAVE – S diperuntukkan untuk organisasi kecil dengan tujuan melakukan investigasi terhadap aset kritis kemudian dibuatkan perencanaan, sedangkan OCTAVE Allegro ditujukan untuk menilai risiko.

## DAFTAR REFERENSI

- [1] "2011 Cybersecurity Watch Survey: Organizations need Skilled Cyber," CERT, Delloit, CSO magazine and US secret service, Framingham, 2011.
- [2] Asian and Pacific Training Center for Information and Communication Technology for Development. (2011, Maret) UN-APCICT. [Online]. <http://www.scribd.com/doc/38458428/13/Tabel-1-1-Perbandingan-Aset-Informasi-dan-Aset-Nyata>
- [3] Dr.Ir.Budi Rahardjo. (2011, Maret) Prinsip Keamanan. ppt.
- [4] Carnegie Mellon University. (2011, Maret) Software Engineering Institute. [Online]. <http://www.cert.org/octave/>
- [5] Audrey J. Dorofee Christopher J. Alberts, "OCTAVE Criteria version 2.0," -, 2001.
- [6] James F. Stevens, Lisa R. Young, William R. Wilson Richard A. Caralli, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," CERT , US, CMU/SEI-2007-TR-012 , May 2007.
- [7] Audrey Dorofee, James Stevens, Carol Woody Christopher Alberts. (2005, Januari) OCTAVE-S Implementation Guide V1. CERT Program.
- [8] Pyka Marek Januszkiwicz Paulina, "Designing a Security Policy According to BS 7799 Using the OCTAVE," *Computer Society*, pp. -, 2007.
- [9] James F. Stevens, "Information Asset Profiling," -, 2005.
- [10] Drew M, "Information Risk Management and Compliance-expect The unexpected," *BT Technology Journal*, vol. Volume 25/Number 1, 2007.
- [11] James F. Stevens, Lisa R. Young, William R. Wilson Richard A. Caralli. (2007, May) The OCTAVE Allegro Guidebook v1.0. CERT Program.