ISSN 2302-8734

Jurnal Teknik

TEKNIK INFORMATIKA - TEKNIK MESIN - TEKNIK SIPIL - TEKNIK ELEKTRO - TEKNIK INDUSTRI

Jurnal Teknik, Vol.3 No. 2, Desember 2014

Fakultas Teknik
Universitas Muhammadiyah Tangerang

Jurnal Teknik ISSN 2302-8734

TEKNIK INFORMATIKA - TEKNIK MESIN - TEKNIK SIPIL - TEKNIK ELEKTRO - TEKNIK INDUSTRI

Susunan Redaksi Jurnal Teknik
Fakultas Teknik - Universitas Muhammadiyah Tangerang

Alamat :
Jl. Perintis Kemerdekaan I No. 33 Cikokol Tangerang 5537198
Telp. : 021 51374916

DAFTAR ISI

MANAJEMEN RISIKO SISTEM INFORMASI PADA PT. ALDIRA BERKAH ABADI MAKMUR DENGAN MENGGUNAKAN METODE OCTAVE-S DAN STANDAR PENGENDALIAN ISO/EIC 27001

Abdurrasyid [1)]
[1)] Jurusan Teknik Informatika
Sekolah Tinggi Teknik PLN
Menara PLN, Jl. Lingkar Luar Barat, Duri Kosambi, Cengkareng, Jakarta Barat
http://ww.sttpln.ac.id
ochidqq@gmail.com

ABSTRAK

Tujuan penulisan adalah agar memberikan pemahaman akan pentingnya analisis risiko bagi perusahaan dan kaitannya dengan bisnis perusahaan, selain itu membantu perusahaan mendapatkan informasi mengenai risiko-risiko, ancaman, serta kelamahan teknologi informasi yang ditemukan dan membantu memberikan solusi dalam melindungi aset-aset informasi perusahaan, dalam bentuk rekomendasi-rekomendasi yang dapat diterapkan oleh perusahaan, Data diambil dari penyebaran kuesioner kepada manajer TI, hasil wawancara, dan observasi pada perusahaan, Data dianalisis dengan menggunakan OCTAVE-S sebagai alat manajemen risiko dan ISO/EIC 27001 disertakan dalam tahap pembuatan mitigasi risiko sebagai standar pengendalian risiko, hasil yang didapatkan dari penelitian yang dilakukan yakni didapatkan SOP apa saja yang harus disusun agar dapat menanggulangi ancaman-ancaman supaya tidak menjadi risiko, didapatkannya suatu hasil penilaian menyeluruh terhadap asset informasi perusahaan terhadap risiko bisnis perusahaan, selain kelemahan, ancaman, serta risiko yang dimiliki perusahaan, didapatkan behwa perusahaan dalam tingkat manajemen risiko sedang, dari penelitian dapat disimpulkan bahwa ancaman yang muncul lebih sering diakibatkan karna kurangnya prosedur operasional standar yang dimiliki perusahaan, sehingga membawa dampak negatif bagi perusahaan, pembuatan dan penerapan SOP akan membantu perusahaan dalam mengurangi permasalahan yang selama ini muncul, sehingga ancaman serta risiko terhadap aset informasi dapat ditekan pada posisi yang lebih rendah.

Kata Kunci: *Keamanan Informasi, Manajemen Risiko, OCTAVE-S, ISO/EIC 27001.*

1. PENDAHULUAN

1.1 Latar Belakang

Maraknya penggunaan teknologi informasi pada perusahaan menempatkan TI kedalam posisi yang sangat diperhatikan, khususnya pada perusahaan besar, apalagi bila TI menjadi bagian *strategic* perusahaan. Begitu pentingnya TI, hingga perusahaan rela mengeluarkan biaya besar demi mendapatkan manfaat yang ditawarkan oleh TI itu sendiri, namun disisi lain muncul kekecewaan akibat investasi yang

dikeluarkan tidak sebanding dengan hasil yang didapat.

Top manajemen selalu menginginkan nilai investasi yang dikeluarkan harus sesuai dengan manfaat yang didapat, tanpa peduli risiko-risiko, ancaman, serta kelemahan yang ada pada perusahaan, khususnya pada hal-hal yang menjadi tanggung jawab divisi TI, yang terkadang tidak disadari dan hal tersebut akan mempengaruhi kinerja bisnis perusahaan baik secara langsung maupun tidak langsung.

Sistem informasi yang ada pada perusahaan sangat membantu baik bisnis unit maupun perusahaan pusat sendiri dalam menjalankan proses bisnis yang berjalan, sistem informasi berubah menjadi aset penting perusahaan, bila sistem informasi terganggu maka akan memberikan dampak buruk bagi perusahaan, dari sisi keuangan sebagai contoh jika sistem otobitz yang berjalan pada bisnis unit PT Rhys terganggu maka akan menimbulkan kerugian, data harga suku cadang disimpan pada sistem tersebut, sehingga akan menghambat bagian kasir untuk melakukan kalkulasi biaya yang harus dibayarkan, selain itu produktifitas karyawan bagian gudang akan menurun dikarnakan tidak ada surat permintaan yang harus dipenuhi akibat sistem yang terganggu, reputasi perusahaan akan terkena dampak berikutnya yang akan menimbulkan kehilangan pelanggan akibat pelayanan yang kurang memuaskan.

Jika ancaman terhadap aset informasi tidak di perhatikan dan tidak dimitigasi membuat ancaman tersebut berubah menjadi risiko yang harus dihadapi oleh perusahaan, disisi lain divisi TI tidak memiliki pengendalian yang dapat membantu dalam menanggulangi kemungkinan ancaman-ancaman yang mungkin muncul dalam proses bisnis perusahaan terkait dengan sistem informasi yang ada pada perusahaan.

Penilaian risiko menjadi langkah yang tepat untuk memberikan pemahaman akan pentingnya kewaspadaan terhadap risiko, ancaman serta kelemahan pada aset informasi yang dimiliki perusahaan, salah satunya penilaian risiko dengan metode *OCTAVE (Operationally Critical Threat, Aset, and Vulnerability Evaluation)*.

Metode *OCTAVE* merupakan salah satu metode yang banyak digunakan oleh perusahaan-perusahaan untuk melakukan penilain risiko. Metode *OCTAVE* sendiri memiliki tiga varian, yaitu *OCTAVE, OCTAVE-S*, dan *OCTAVE Allegro*. Adapun metode yang digunakan dalam penulisan ini adalah metode *OCTAVE-S*, dimana metode ini merupakan modifikasi dari metode *OCTAVE* yang disesuaikan dengan kapasitas perusahaan. *OCTAVE-S,* dimana penggunaan *OCTAVE-S* lebih umum ditujukan untuk menganalisa risiko pada perusahaan yang memiliki skala kecil hingga menengah dengan jumlah staf yang kurang dari 300, dan memungkinkan aktifitas analisis risiko dilakukan oleh tim dalam jumlah kecil.

Adapun ISO/EIC 27001 merupakan merupakan standar Internasional yang dipersiapkan untuk memberikan model untuk membangun, mengimplementasikan, mengoperasikan, memonitor, serta merawat dan mengembangkan sistem manajemen keamanan informasi (SMKI), metode ini akan digunakan sebagai acuan dalam menentukan pengendalian, setelah penilaian risiko dilakukan denga menggunakan OCTAVE-S.

PT. Aldira Berkah Abadi Makmur merupakan *holding company* yang memiliki beberapa bisnis unit yang bergerak diberbagai bidang, dengan jumlah karyawan kurang dari 300 orang, baik *holding* maupun bisnis unit dalam menjalankan operasional harian semuanya tidak lepas dari penggunaan teknologi informasi sebagai alat bantu untuk meningkatkan efisiensi

dan efektifitas agar perusahaan menjadi lebih kompetitif.

Didasari dari latar belakang yang dipaparkan diatas didukung dengan belum pernahnya dilakukan penilaian risiko teknologi informasi, khususnya dengan menggunakan metode *OCTAVE-S*, ditambah kesesuaian spesifikasi perusahaan dengan metode yang dipilih, menjadi alasan dilakukannya penilaian risiko pada PT. Aldira Berkah Abadi Makmur.

1.2 Rumusan Permasalahan

Rumusan permasalahan yang mendasari dilakukannya penilaian risiko pada PT Aldira Berkah Abadi Makmur adalah:

1. Kurangnya *standard operational procedure* (SOP) yang mengacu kepada tindakan dalam menjaga keamanan teknologi informasi yang ada pada perusahaan. Pengaruh yang ditimbulkan adalah ketidaksigapan dalam menanggulangi risiko-risko serta ancaman yang muncul dan harus ditangani secara cepat dan tepat sehingga mengakibatkan terganggunya operasional perusahaan.
2. Kurangnya dokumentasi-dokumentasi yang berkenaan penilaian akan pentingnya nilai dari aset informasi yang dimiliki oleh perusahaan.

1.3 Tujuan dan manfaat

Tujuan penulisan ini adalah:

1. memberikan pemahaman akan pentingnya analisis risiko bagi perusahaan dan kaitannya dengan bisnis perusahaan.
2. Membantu PT. Aldira Berkah Abadi Makmur dengan memberikan informasi kepada perusahaan mengenai risiko-risiko, ancaman, serta kelemahan teknologi informasi yang ditemukan.
3. Membantu memberikan solusi dalam melindungi aset-aset informasi perusahaan, dalam bentuk rekomendasi-rekomendasi yang dapat diterapkan oleh PT. Aldira Berkah Abadi Makmur.

Manfaat yang ingin dicapai dalam penelitian ini adalah:

1. Teridentifikasinya permasalahan yang ada pada sistem informasi PT. Aldira Berkah Abadi Makmur.
2. Dokumen akhir dapat dijadikan sebagai pedoman dan membantu dalam pengembangan penilaian analisis risiko kedepannya.
3. Menghasilkan rancangan dan solusi yang dapat membantu perusahaan berkaitan dengan pengelolaan risiko sehingga dapat membantu perusahaan dalam mengatasi masalah yang muncul, dan meminimalisir celah kelemahan pada perusahaan PT. Aldira Berkah Abadi Makmur berdasarkan standar yang diacu yakni *OCTAVE-S* dan ISO/IEC 27001.
4. Timbulnya kesadaran akan pentingnya manajemen risiko sistem informasi bagi perusahaan.
5. Pihak manajemen dapat secara efektif mengkomunikasikan nilai-nilai penting informasi keamanan informasi, yang didukung dengan data-data yang telah didapat.

1.4 Ruang Lingkup

Ruang lingkup dalam penelitian ini adalah sebagai berikut:

1. Pelaksanaan proses manajemen risiko dilakukan di perusahaan PT Aldira Berkah Abadi Makmur.
2. Pelaksanaan proses manajemen risiko dilakukan pada divisi teknologi informasi, PT Aldira Berkah Abadi Makmur.
3. Metode yang digunakan dalam melakukan penilaian risiko adalah metode *OCTAVE-S.*

4. Adapun metode pengendalian yang digunakan mengacu kepada standar ISO / EIC 27001:2005.
5. Penelitian ini pada akhirnya akan menghasilkan dokumen-dokumen yang berisikan, penilaian risiko serta rekomendasi pengendalian atas risiko yang telah didefinisikan sebelumnya.

2. LANDASAN TEORI

2.1 Sistem Informasi

(Laudon & Laudon, 2009) menjelaskan bahwa sistem informasi itu merupakan bagian integral dari organisasi yang terdiri atas tiga komponen yaitu:

1) Organisasi, perusahaan-perusahaan bisnis merupakan organisasi formal yang terdiri atas unit-unit khusus dengan pembagian devisi yang jelas. Organisasi butuh membangun sistem untuk mengatasi permasalahan yang terbentuk baik yang berasal dari faktor internal maupun faktor eksternal.
2) Manusia, orang-orang menggunakan informasi dari sistem berbasis komputer dalam pekerjaan mereka, dan mengintegrasikannya ke dalam lingkungan pekerjaan. Mereka memasukkan data (input) kesistem baik oleh mereka sendiri ataupun melalui perantara atau media yang dapat dibaca oleh komputer.
3) Teknologi, teknologi adalah suatu alat dimana data ditransformasikan dan diorganisasikan untuk kemudian digunakan manusia. Komputer telah menggantikan teknologi manual dengan melakukan pemprosesan atas data yang jumlahnya sangat besar, ataupun menjalankan pekerjaan yang sangat komplek. Komputer juga dapat bekerja secara konsisten serta reliabel (dapat dipercaya) dalam waktu yang lebih lama bila dibanding dengan kemampuan manusia.

2.2 Keamanan Informasi

Begitu bernilainya suatu informasi bagi suatu organisasi atau perusahaan, hingga perlu untuk diamankan, Alberts & Dorofee (2003) menjelaskan bahwa keamanan informasi tidak hanya sekedar melakukan instalasi *firewall*, kemudian perbaikan pada perangkat lunak disaat terjadi masalah, kemudian mengunci rapat-rapat lemari arsip sehingga tidak dapat diambil oleh orang yang tidak berhak. Namun kemanan informasi adalah pemahaman akan apa yang harus kita lindungi, dan mengapa hal tersebut harus kita lindungi, kemudian mengidentifikasi ancaman apa yang dapat mengganggu hal yang kita lindungi tersebut, dan menentukan langkah apa yang harus dilakukan untuk melindunginya.

Ancaman merupakan tindakan-tindakan yang dapat menimbulkan kerusakan, kehilangan atau hal lain yang memberikan dampak buruk, dan ancaman-ancaman keamanan yang muncul akan berubah menjadi risiko jika tidak ditanggulangi dengan cepat dan tepat (Young, 2010), diperkuat lagi oleh Caralli (2007) yang menyatakan ancaman adalah indikasi dari kemungkinan munculnya kejadian yang tidak diharapkan. ancaman mengacu kepada situasi (atau skenario) dimana seseorang dapat melakukan tindakan yang tidak diharapkan (contohnya seorang penyerang mengrimkan trojan kedalam komputer server akibat mengunduh data dari situs yang diragukan) atau kejadian alam yang dapat menyebabkan hasil yang tidak diinginkan (sebagai contoh gempa bumi yang dapat merusak infrastruktur sistem informasi perusahaan).

Bagi perusahaan yang menempatkan informasi sebagai aset berharga, tidak akan segan untuk mengeluarkan biaya besar untuk menjaga asetnya selama biaya tersebut sesuai dengan dampak terhadap bisnis, karena menurut survey yang dilakukan oleh Ernst & Young's (2008)

dampak yang paling besar dari terganggunya informasi perusahaan adalah:

1) *Brand image,* reputasi perusahaan.
2) Hilangnya kepercayaan diri dari para stakeholder.
3) Hilangnya keuntungan financial.
4) Hilangnya pelanggan.
5) Sanksi regulasi.

Menurut Satti, Nagrial, & Garner (2002) terdapat 10 aspek keamanan informasi yakni

1) **Kebijakan Keamanan**: untuk memberikan arahan dan dukungan manajemen keamanan informasi. Manajemen harus menetapkan arah kebijakan yang jelas dan menunjukkan dukungan, serta komitmen terhadap keamanan informasi melalui penerapan dan pemeliharaan suatu kebijakan keamanan informasi di seluruh tataran organisasi.
2) **Pengorganisasian Keamanan**: untuk mengelola keamanan informasi dalam suatu organisasi. Satu kerangka kerja manajemen harus ditetapkan untuk memulai dan mengkontrol penerapan keamanan informasi di dalam organisasi.Manajemen dengan kepemimpinan yang kondusif harus dibangun untuk menyetujui kebijakan keamanan informasi, menetapkan peran keamanan dan mengkoordinir penerapan keamanan di seluruh tataran organisasi. Jika diperlukan, pendapat pakar keamanan informasi harus dipersiapkan dan tersedia dalam organisasi. Hubungan dengan pakar keamanan eksternal harus dibangun untuk mengikuti perkembangan industri, memonitor standar dan metode penilaian serta menyediakan penghubung yang tepat, ketika berurusan dengan insiden keamanan. Pendekatan multi-disiplin terhadap keamanan informasi harus dikembangkan, misalnya dengan melibatkan kerjasama dan kolaborasi di antara manajer, pengguna, administrator, perancang aplikasi, pemeriksa dan staf keamanan, serta keahlian di bidang asuransi dan manajemen risiko.
3) **Klasifikasi dan Kontrol Aset**: untuk memelihara perlindungan yang tepat bagi pengorganisasian aset. Semua aset informasi penting harus diperhitungkan keberadaannya dan ditentukan kepemilikannya. Akuntabilitas terhadap aset akan menjamin terdapatnya perlindungan yang tepat. Pemilik semua aset penting harus diidentifikasi dan ditetapkan tanggung jawabnya untuk memelihara sistem kontrol tersebut. Tanggungjawab penerapan sistem kontrol dapat didelegasikan. Akuntabilitas harus tetap berada pada pemilik aset.
4) **Pengamanan Personil**: untuk mengurangi risiko kesalahan manusia, pencurian, penipuan atau penyalahgunaan fasilitas. Tanggung jawab keamanan harus diperhatikan pada tahap penerimaan pegawai, dicakup dalam kontrak dan dipantau selama masa kerja pegawai.
5) **Keamanan Fisik dan Lingkungan**: untuk mencegah akses tanpa otorisasi, kerusakan, dan gangguan terhadap tempat dan informasi bisnis. Fasilitas pemrosesan informasi bisnis yang penting dan sensitif harus berada di wilayah aman, terlindung dalam perimeter keamanan, dengan rintangan sistem pengamanan dan kontrol masuk yang memadai. Fasilitas tersebut harus dilindungi secara fisik dari akses tanpa ijin, kerusakan dan gangguan. Perlindungan harus disesuaikan dengan identifikasi risiko.
6) **Komunikasi dan Manajemen Operasi**: untuk menjamin bahwa fasilitas pemrosesan informasi berjalan dengan

benar dan aman. Harus ditetapkan tanggungjawab dan prosedur untuk manajemen dan operasi seluruh fasilitas pemrosesan informasi. Hal ini mencakup pengembangan instruksi operasi yang tepat dan prosedur penanganan insiden. Dimana mungkin harus ditetapkan pemisahan tugas untuk mengurangi risiko penyalahgunaan sistem karena kecerobohan atau kesengajaan.

7) **Pengontrolan Akses**: untuk mencegah akses tanpa ijin terhadap sistem informasi. Prosedur formal harus diberlakukan untuk mengkontrol alokasi akses, dari pendaftaran awal dari pengguna baru sampai pencabutan hak pengguna yang sudah tidak membutuhkan lagi akses ke sistem informasi dan layanan. Perhatian khusus harus diberikan, jika diperlukan, yang dibutuhkan untuk mengkontrol alokasi hak akses istimewa, yang memperbolehkan pengguna untuk menembus sistem kontrol.
8) **Pengembangan dan Pemeliharaan Sistem**: untuk memastikan bahwa keamanan dibangun dalam sistem informasi. Persyaratan Keamanan sistem mencakup infrastruktur, aplikasi bisnis dan aplikasi yang dikembangkan pengguna. Disain dan implementasi proses bisnis yang mendukung aplikasi atau layanan sangat menentukan bagi keamanan. Persyaratan keamanan harus diidentifikasi dan disetujui sebelum pengembangan sistem informasi. Semua persyaratan keamanan sisitem informasi, termasuk kebutuhan pengaturan darurat, harus diidentifikasi pada fase persyaratan suatu proyek, dan diputuskan, disetujui serta didokumentasikan sebagai bagian dari keseluruhan kasus bisnis sebuah sistem informasi.
9) **Manajemen Kelangsungan Bisnis**: Untuk menghadapi kemungkinan penghentian kegiatan usaha dan melindungi proses usaha yang penting dari akibat kegagalan atau bencana besar. Proses manajemen kelangsungan usaha harus diterapkan untuk mengurangi kerusakan akibat bencana atau kegagalan sistem keamanan (yang mungkin dihasilkan dari, sebagai contoh, bencana alam, kecelakaan, kegagalan alat dan keterlambatan) sampai ke tingkat yang dapat ditolerir melalui kombinasi pencegahan dan pemulihan kontrol. Konsekuensi dari bencana alam, kegagalan sistem keamanan dan kehilangan layanan harus dianalisa. Rencana darurat harus dikembangkan dan diterapkan untuk memastikan proses usaha dapat disimpan ulang dalam skala waktu yang dibutuhkan. Rencana semacam itu harus dijaga dan dipraktekkan untuk menjadi bagian integral keseluruhan proses manajemen. Manajemen kelangsungan bisnis harus mencakup kontrol untuk mengidentifikasi dan mengurangi risiko, membatasi konsekuensi kesalahan yang merusak, dan memastikan penyimpulan tahapan operasional yang penting; dan
10) **Kesesuaian**: Untuk menghindari pelanggaran terhadap hukum pidana maupun hukum perdata, perundangan, peraturan atau kewajiban kontrak serta ketentuan keamanan lainnya. Disain, operasional, penggunanan dan manajemenan sistem informasi adalah subyek dari perundangan, peraturan, dan perjanjian kebutuhan keamanan. Saran untuk kebutuhan legalitas yang bersifat khusus harus dicari dari penasihat hukum organisasi, atau praktisi hukum yang berkualitas.

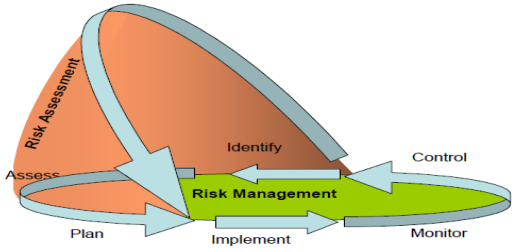
2.3 Risiko

Menurut Kloman (2000), kata *"risk"* dalam bahasa Inggris berasal dari bahasa Italia kuno yaitu *"riscare".* Risiko mempunyai definisi yang begitu beragam dengan begitu banyak pengertian dan interpretasi, tergantung dari cara orang memandangnya. Risiko dapat dipandang sebagai:

a. Sesuatu yang merugikan terjadi *(risk of loss)*
b. Suatu ketidakpastian *(risk of volatility)*
c. Sesuatu yang menguntungkan tidak terjadi *(risk of lost opportunity).*

2.4 Manajemen Risiko dan Penilaian Risiko

Manajemen risiko dan penilaian risiko merupakan komponen penting dalam manajemen sistem informasi, menurut *Technical Department of European Network and Information Security Agency* (ENISA) (2006) manajemen risiko merupakan proses, berbeda dari penilaian risiko, menimbang kebijakan alternatif dalam konsultasi dengan pihak yang berkepentingan, mempertimbangkan penilaian risiko dan faktor sah lainnya, dan, memilih pencegahan yang tepat serta pilihan kontrol.



Gambar 1 Hubungan antara manajemen risiko dan penilaian risiko (ENISA, 2006).

2.5 Proses Manajemen Risiko

Menurut ENISA (2006) efektif tidaknya penerapan manajemen risiko pada suatu organisasi atau perusahaan, tergantung pada budaya organisasi itu sendiri karena manajemen risiko merupakan tanggung jawab semua bagian dari organisasi. Biasanya dalam mendesain dan mengimplementasikan proses manajemen risiko pada setiap organisasi dipengaruhi oleh:

a) Misi dan tujuan organisasi.
b) Produk dan layanan yang ditawarkan organisasi.
c) Manajemen dan proses operasional organisasi.
d) Praktek-praktek khusus yang diterapkan.
e) Regulasi serta lingkungan yang berlaku dimana organisasi itu berada.

Tsohou, Karyda, Kokolakis, & Kiountouzis (2006) menyatakan bahwa secara umum proses manajemen risiko tidak terlepas dari tiga hal

1) Inisiasi (*Initiation*).

Tahap utama yang dilakukan saat inisiasi adalah:

a. mendefinisikan konteks dari proses manajemen risiko.
b. Menentukan cakupan analisis.
c. Membuat tim untuk melakukan manajemen risiko.

2) Analisa Risiko (*Risk Analysis*)

Pada tahap analisis risiko terdapat tiga proses yang harus dilakukan:

a. Identifikasi risiko.

Pada tahap ini dilakukan identifikasi risiko yang dapat menimbulkan ancaman terhadap aset-aset yang harus dilindungi, identifikasi kelemahan-kelemahan yang ada.

b. Estimasi risiko.

Risiko-risiko yang telah diidentifikasi kemudian diukur dan dinilai berdasarkan tingkat kemungkinan, serta dampak bisnis atau biaya yang akan dikeluarkan jika risiko terjadi.

c. Evaluasi risiko

Setelah risiko yang ada telah diidentifikasi maka dilakukan evaluasi untuk menentukan tingkat toleransi, sehingga

dapat diambil keputusan apakah risko akan diambil, ditransfer kepada pihak ketiga, dihindari secara keseluruhan, atau direduksi dengan menyeleksi risiko-risiko sesuai dengan kemampuan.

3) Mitigasi Risiko(Risk Mitigation)

Mengacu kepada ISO/IEC 27001 (2005) terdapat tiga langkah yang harus dilakukan pada tahap ini ketiga tahap itu adalah:

a. Desain

Proses mitigasi risiko mencakup spesifikasi tujuan keamanan dan pembentukan kebijakan keamanan serta proses yang relevan untuk mengendalikan risiko. kebijakan serta penanggulangan ada diidentifikasi dan dievaluasi serta dibandingkan dengan hasil analisis risiko. Jika diperlukan, dibuat langkah-langkah kontrol tambahan serta waktu pelaksanaannya.

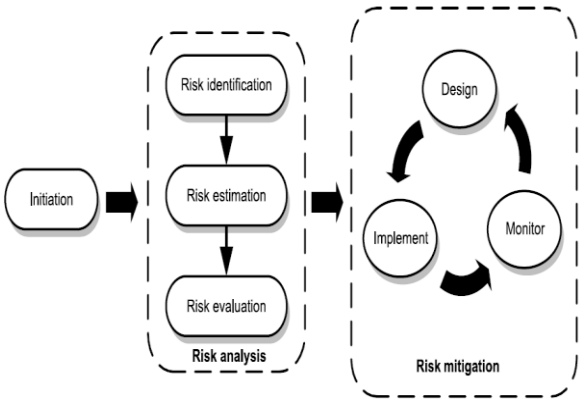
b. Implementasi

Proses implementasi melibatkan penerapan dari prosedur dan tindakan kendali yang dipilih termasuk juga pengelolaan aspek lain yang mendukung kesuksesan implementasi pengendalian risiko. Program kesadaran keamanan juga termasuk dalam proses ini, bertujuan untuk menanggulangi risiko yang ada dan membangun budaya keamanan.

c. Pemantauan

Pada tahap pemantauan ini hal yang dilakukan adalah sebagai berikut:

a) Pemantauan dalam mendeteksi kesalahan dengan cepat serta insiden keamanan.
b) Pemantauan terhadap mekanisme apakah prosedur yang terdokumentasi dijalankan sebagaimana mestinya.
c) Ulasan mengarah pada evaluasi efisiensi kontrol diimplementasikan



Gambar 2 Proses manajemen risiko secara umum (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2006)

2.6 *OCTAVE*

OCTAVE adalah metodologi yang dikembangkan oleh institusi rekayasa perangkat lunak universitas Carnagie Mellon, digunakan untuk melakukan penilaian risiko yang menggabungkan antara analisis prilaku organisasi, dan kelemahan-kelemahan teknologi. Komponen penting *OCTAVE* adalah tim penganalisa dapat dibangun dari internal perusahaan itu sendiri yang memiliki keterampilan teknis serta keterampilan organisasi yang terkait dengan praktek-praktek bisnis (Coleman, 2004).

Pendekatan *OCTAVE* didasari pada dua aspek:

1) Risiko Operasional
2) Praktek-praktek kemanan

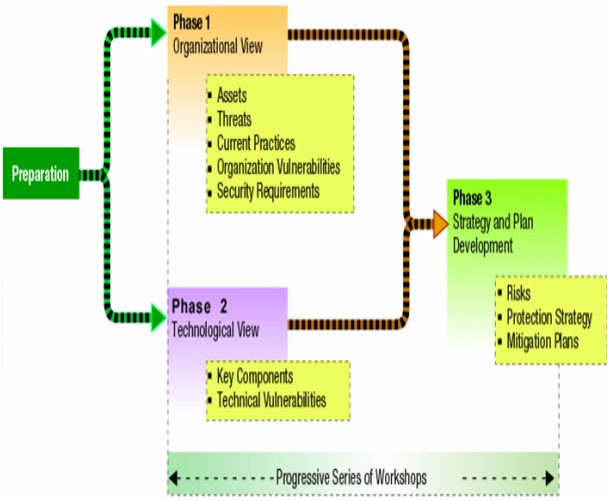
2.6.1. Variasi Metode OCTAVE

Hingga saat ini (Januari 2012) terdapat tiga terdapat varian *OCTAVE* yang bisa digunakan. Ketiga varian tersebut adalah:

1. *OCTAVE*

Metode *OCTAVE* merupakan versi *OCTAVE* yang pertama kali dikembangkan. Metode OCTAVE adalah sebuah pendekatan untuk mengevaluasi risiko keamanan informasi secara komprehensif, sistematis, *context-driven*, and *self-directed*. Pendekatan ini diwujudkan dalam seperangkat

kriteria yang mendefinisikan unsur-unsur penting dari evaluasi keamanan informasi berdasarkan aset. Metode *OCTAVE* ditujukan untuk analisis risiko terhadap perusahaan besar yang memiliki 300 atau lebih karyawan. *OCTAVE* memilki tiga fase seperti ditunjukan oleh gambar tiga dibawah.



Gambar 3 Langkah-langkah OCTAVE (Carol Woody, 2006)

2. *OCTAVE-S*

OCTAVE-S merupakan variasi dari *OCTAVE* yang digunakan untuk melakukan evaluasi terhadap perusahaan kecil, yang memiliki struktur hirarki organisasi yang sedikit, atau memenuhi kriteria sebagai berikut:

a. Fungsi-fungsi teknologi informasi dilakukan secara outsource.
b. Memiliki infrastruktur teknologi informasi yang relatif sederhana yang dapat dimengerti paling tidak oleh satu orang dalam organisasi.
c. Keterbatasan pemahaman mengenai alat yang dapat digunakan untuk evaluasi risiko terhadap aset informasi.
d. Organisasi lebih menyukai metode yang sangat terstruktur dibandingkan metode terbuka yang dapat lebih mudah disesuaikan.

Output yang dihasilkan *OCTAVE-S* sama dengan *OCTAVE*. *OCTAVE-S* memiliki fase yang sama dengan *OCTAVE* hanya saja memiliki jumlah aktifitas yang lebih sedikit dibandingkan dengan *OCTAVE*, namun tidak mengurangi kompleksitas dari evaluasi risiko yang ada, karena *OCTAVE-S* dilengkapi juga dengan konsep-konsep keamanan serta panduannya, yang memungkinkan orang yang tidak memiliki pengalaman dapat melakukan evaluasi dengan benar berdasarkan panduan yang ada (Alberts, Dorofee, Stevens, & Woody, 2005).

3. *OCTAVE Allegro*.

Tujuan yang ingin dicapai oleh *OCTAVE Allegro* adalah penilaian yang luas terhadap lingkungan risiko operasional suatu organisasi dengan tujuan menghasilkan penilaian tanpa perlu pengetahuan yang luas dalam hal penilaian risiko. Pendekatan ini berbeda dari pendekatan *OCTAVE*, dimana *OCTAVE Allegro* lebih berfokus terhadap aset informasi dalam konteks bagaimana mereka digunakan, dimana mereka disimpan, dipindahkan, dan diolah, dan bagaimana mereka terkena ancaman, kerentanan, dan gangguan sebagai hasil yang ditimbulkan (Caralli, Stevens, Young, & Wilson, 2007).

2.7 ISO/EIC 27001:2005

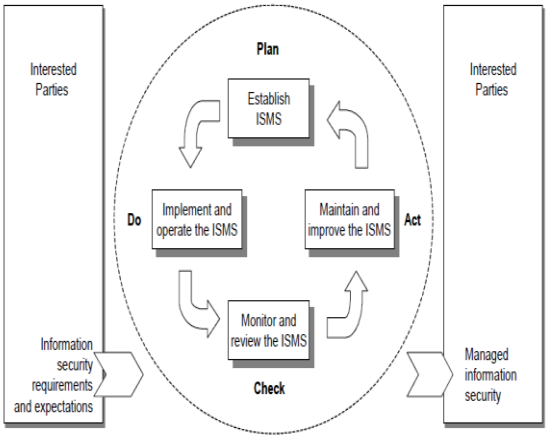
ISO (*the International Organization for Standardization*) and EIC (*the International Electrotechnical Commission*) merupakan lembaga internasional yang aktif mengeluarkan standar-standar bagi operasional organisasi yang diakui oleh setidaknya 75% dari total negara yang ada didunia.

ISO/EIC 27001:2005 merupakan standar Internasional yang dipersiapkan untuk memberikan model untuk membangun, mengimplementasikan, mengoperasikan, memonitor, serta merawat dan mengembangkan sistem manajemen keamanan

informasi (SMKI) (ISO & EIC, 2005).

ISO / IEC 27001 telah dikembangkan untuk melindungi aset informasi suatu organisasi, "'darah kehidupan' dari semua bisnis" (Humfreys, 2005). Ada beberapa faktor pemicu diadopsinya ISO/IEC 27001, dimana secara internal perusahaan akan terciptanya kesadaran akan kerentanan SI dan proses penting perusahaan (Barlette, 2006). Faktor pendorong lain diadopsinya ISO/IEC 27001:2005 adalah untuk menunjukan kepada mitra kerja bahwa perusahaan telah mengidentifikasi dan mengukur keamanan risiko perusahaan dan menerapkan kebijakan keamanan dan kontrol yang dapat mengurangi risiko, sehingga memberikan keyakinan yang kuat terhadap perusahaan tersebut (Saint-Germain, 2005), disamping itu ada pula yang menjadikan ISO/IEC 27001:2005 sebagai kebijakan pemerintah seperti di Jepang, atau suatu keharusan bagi perusahaan *outsource* seperti Taiwan, Singapura, serta India (Backhouse, Hsu, & Silva, 2006).

ISO mengadopsi model *plan-do-check-act* (PDCA) sebagai proses dari SMKI yang digunakan seperti ditunjukan pada gambar 4 dibawah ini Model SMKI ISO



Gambar 4 Model PDCA diaplikasikan pada proses SMKI (ISO & EIC, 2005)

1) *Plan*
   Menetapkan kebijakan SMKI, tujuan, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi untuk memberikan hasil yang sesuai dengan kebijakan dan tujuan organisasi.
2) *Do*
   Menerapkan dan mengoperasikan kebijakan SMKI, kontrol, proses dan prosedur.
3) *Check*
   Menilai dan, mengukur kinerja proses terhadap kebijakan SMKI, tujuan dan pengalaman praktis serta melaporkan hasilnya kepada manajemen untuk ditinjau ulang.
4) *Act*
   Mengambil tindakan perbaikan dan pencegahan, berdasarkan hasil audit internal SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan secara terus-menerus dari SMKI. (ISO & EIC, 2005)

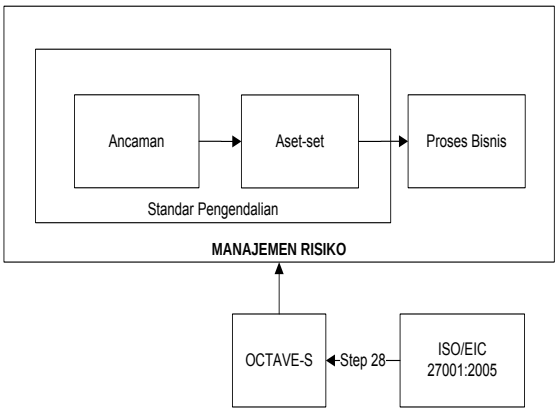
Dalam membangun dan mengelola SMKI ada empat hal yang harus dilakukan menurut ISO / EIC 27001 yaitu:

1) Organisasi diharuskan untuk mendefinisikan dan mendokumentasikan metode penilaian risiko yang digunakan. (Brenner, 2007)
2) Mengimplementasikan dan menjalankan SMKI.
3) Melakukan pemantauan dan peninjauan ulang terhadap SMKI yang telah berjalan.
4) Merawat dan terus mengembangkan SMKI di dalam organisasi, dan pastikan pengembangan yang dilakukan harus memenuhi tujuan perusahaan.

3. METODOLOGI PENELITIAN

3.1 Kerangka pikir

Kerangka pikir dalam penelitian ini dapat digambarkan seperti dibawah:



Gambar 5 Kerangka Pikir

Ancaman merupakan tindakan-tindakan yang dapat menimbulkan kerusakan, kehilangan atau hal lain yang memberikan dampak buruk, dan ancaman-ancaman keamanan yang muncul akan berubah menjadi risiko jika tidak ditanggulangi dengan cepat dan tepat (Young, 2010) .

Ancaman akan menjadi risiko yang harus diterima perusahaan jika tidak dimitigasi , dimana ancaman melekat pada aset perusahaan baik itu aset informasi maupun aset sumberdaya manusia, atau aset-aset yang lainnya, untuk itu perusahaan harus memahami ancaman-ancaman apa saja yang mungkin muncul yang dapat mengganggu aset penting sehingga dapat mempengaruhi proses bisnis yang berdampak pada kerugian bagi perusahaan.

Aset perusahaan merupakan bagian penting dalam menjalankan proses bisnis perusahaan, terlebih lagi aset penting perusahaan baik berupa aset informasi, sumber daya manusia, maupun aset lainnya, aset penting harus dilindungi dan dirawat sebaik-baiknya agar tidak mengganggu proses bisnis, sehingga tidak memberikan dampak buruk bagi perusahaan.

Untuk itu aset perusahaan harus didefinisikan dan dikaitkan dengan ancaman-ancaman yang mungkin dapat mempengaruhi aset-aset tersebut, selain itu juga memudahkan perusahaan untuk mengetahui seberapa besar aset-aset yang dimiliki perusahaan khususnya aset informasi.

Ancaman yang mempengaruhi aset terlebih lagi yang tidak dimitigasi dapat berubah menjadi risiko bagi perusahaan, dan akan mempengaruhi proses bisnis perusahaan, baik itu mengakibatkan menurunnya produktifitas karyawan, atau bahkan membuat proses bisnis berhenti disebabkan gangguan yang ditimbulkan oleh ancaman yang tidak diidentifikasi dan tidak dimitigasi.

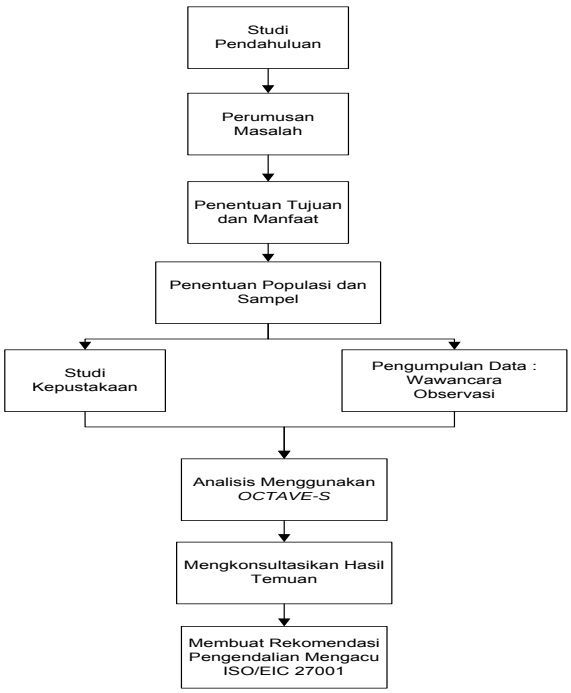
Untuk itu perlu dilakukan manajemen risiko yang ditujukan untuk mendefinisikan aset apa saja yang dimiliki oleh perusahaan khususnyan aset informasi, selain itu guna mengetahui ancaman-ancaman apa saja yang dapat mempengaruhi atau mengganggu kinerja aset perusahaan, yang dapat menimbulkan kekacauan baik itu dalam skala kecil, menengah hingga memberikan dampak kerugian yang tinggi bagi perusahaan, selain itu memberikan informasi akan dampak dari ancaman terhadap proses bisnis perusahaan, serta bagaimana cara agar aset-aset penting perusahaan tidak terganggu setidaknya tidak menimbulkan dampak buruk bagi kelangsungan bisnis perusahaan.

Untuk melakukan manajemen risiko maka diperlukan alat standar yang dapat digunakan untuk melakukan hal-hal yang telah disebutkan diatas, maka digunakanlah *octave* sebagai alat untuk melakukan manajemen risiko, dimana octave sendiri telah digunakan oleh berbagai institusi baik swasta maupun pemerintah, dan digunakan oleh berbagai Negara , selain itu octave memiliki kelebihan tersendiri

dimana memiliki varian yang dapat digunakan khusus untuk perusahaan dengan skala kecil atau memiliki criteria perusahaan yang sesuai dengan karakteristik octave-s dan itu sesuai dengan perusahaan PT Aldira Berkah Abadi Makmur.

Tidak hanya itu untuk melengkapi octave-s diperlukan pula mitigasi standar yang tepat agar hasil yang didapatkan saat dilakukan evaluasi dari penerapan manajemen risiko memuaskan, octave-s memiliki 30 tahap dimana pada tahap ke 28 terdapat proses pembuatan mitigasi terhadap ancaman-ancaman yang sudah didefinisikan pada tahap-tahap sebelumnya, untuk menyempurnakan pembuatan mitigasi pada step 28 maka disertakan ISO/EIC 27001:2005, dipakai sebagai standar pengendalian yang dipetakan dengan ancaman-ancaman terhadap aset yang didapatkan sebelumnya.

3.2. Rencanan Penelitian



Gambar 6. Rencana Penelitian

3.2.1. Studi pendahuluan

Pada tahap ini, menggambarkan proses awal sebelum penelitian dilakukan, yang dimulai dari pengajuan proposal untuk melakukan penelitian yang ditujukan kepada perusahaan. Pada tahap ini pula komunikasi awal dilakukan dengan pihak perusahaan, dalam hal ini adalah PT. Aldira Berkah Abadi Makmur, adapun yang dituju adalah manajer TI perusahaan, sebagai struktur tertinggi yang bertanggung jawab terhadap segala hal yang berkaitan dengan teknologi informasi perusahaan. Dibicarakan mengenai ide, gambaran umum mengenai ide yang hendak di wujudkan, serta langkah-langkah apa saja yang akan dilakukan dalam penelitian, hingga didapatkan kesepakatan dalam bentuk penandatanganan proposal yang diajukan. Langkah selanjutnya adalah mempelajari struktur organisasi PT. Aldira Berkah Abadi Makmur dan menentukan dan mengajukan aktor-aktor yang akan membantu selama proses manajemen risiko berlangsung, selain itu mempelajari proses bisnis, sistem, serta infrastruktur informasi yang berjalan di perusahaan.

3.2.2. Perumusan Masalah

Perumusan masalah dilakukan agar penelitian yang dilakukan tidak melebar, yang akan membuat penelitian menjadi tidak terarah, maka perlu dilakukan identifikasi permasalahan yang hendak dibantu penyelesesaiannya.

3.2.3. Tujuan dan Manfaat yang Ingin Dicapai

Pada tahapan ini ditentukan dan diperjelas mengenai manfaat dan tujuan dari penelitian yang hendak dilakukan, agar penelitian yang dilakukan menjadi bermakna bagi perusahaan khususnya, maupun bagi dunia pendidikan secara umum.

3.2.4. Penentuan Populasi dan Sampel

Populasi yang akan dijadikan sebagai objek adalah karyawan PT. Aldira Berkah Abadi Makmur yang berada dikantor pusat, pemilihan ini dikarnakan karyawan terbanyak bekerja di kantor pusat, dimana di kantor pusat terdapat dua bisnis unit yang menyatu dalam satu gedung, sehingga jumlah karyawannya lebih besar dibandingkan dengan di bisnis unit yang berada di luar gedung pusat.

Sampel yang diambil berjumlah 13 orang berisikan seluruh divisi TI yang berjumlah lima orang, ditambah delapan orang non TI yang terdiri dari satu general manajer HRD, satu manajer HRD, satu manajer internal audit, satu general manajer *accounting*, satu manajer *accounting*, satu manajer bisnis unit PT. Rhys, dan dua manajer bisnis unit PT. Andi-Arta. Dengan pemilihan ini diharapkan dapat mewakili seluruh karyawan yang ada di perusahaan PT. Aldira Berkah Abadi Makmur.

3.2.5. Studi Kepustakaan

Pada tahap ini dilakukan pembelajaran, pemahaman, serta pendalaman terhadap literatur-literatur yang telah dikumpulkan sebelumnya pada tahap awal, baik berupa jurnal, tesis, buku, maupun panduan yang dikeluarkan oleh organisasi resmi yang kompeten dalam melakukan proses manajemen risiko pada suatu perusahaan , dan dijadikan sebagai acuan dalam melakukan penelitian, dalam hal ini khususnya yang berkaitan dengan metode *OCTAVE-S* dan ISO/EIC 27001.

3.2.6. Pengumpulan data

Tahap ini dilakukan sejalan dengan tahap sebelumnya, dilakukan pengumpulan data dengan cara:

a. Observasi

Mengamati dengan teliti bagaimana proses yang berjalan di perusahaan PT. Aldira Berkah Abadi Makmur, melihat aset-aset informasi yang dimiliki perusahaan dan menghubungkaitkan dengan kemungkinan munculnya risiko.

Selain itu pada tahap ini dilakukan pengumpulan dokumen-dokumen yang yang ada seperti kebijakan tertulis terkait dengan manajemen sistem informasi, pengendalian-pengendalian yang ada, dokumentasi sistem yang berjalan, gambaran infrastruktur teknologi informasi perusahaan, laporan hasil penilaian manajemen risiko sebelumnya jika pernah dilakukan, laporan hasil audit (jika ada) serta dokumen lain yang dapat dijadikan sebagai dasar awal untuk melihat kondisi awal manajemen risiko di PT. Aldira Berkah Abadi Makmur.

b. Wawancara

Melakukan pengumpulan data yang dilakukan dengan memberikan pertanyaan kepada aktor-aktor yang telah disebutkan sebelumnya, sehingga dapat memberikan gambaran umum mengenai kondisi awal manajemen risiko perusahaan.

3.2.7. Analisis Menggunakan Metode OCTAVE-S

Terdapat tiga tahapan utama dalam metode *OCTAVE-S*, yaitu:

a. Membuat profil aset beserta ancaman-ancamannya
b. Mengidentifikasi kelemahan-kelemahan infrastruktur
c. Membuat rancangan keamanan strategi

Lebih jelasnya mengenai metode OCTAVE-S, akan dibahas pada sub bab 3.5.

3.2.8. Mengkonsultasikan Hasil Temuan

Pada tahap ini hasil dari penilaian, temuan risiko serta kelemahan-kelemahan yang ada disampaikan kepada pihak perusahaan, agar memahami setiap hal yang

telah dilakukan dan mengetahui bagaimana hasil dari kegiatan penilaian yang telah dilakukan.

3.2.9. Membuat Rekomendasi Pengendalian Mengacu ISO/EIC 27001:2005

Pada tahap 28 octave-s yakni membuat rencana mitigasi risiko, dibuat rekomendasi-rekomendasi yang berguna untuk memitigasi ancaman yang dapat memberikan dampak buruk terhadap asset informasi perusahaan, agar mitigasi yang dibuat menjadi lebih terarah dan memiliki standar yang baik maka disertakan ISO/EIC 27001:2005, yang merupakan standar pengendalian risiko spesifik terhadap sistem informasi dan telah diakui di lebih dari 20 negara besar didunia, dengan dipadukannya antara OCTAVE-S dan ISO/EIC 27001:2005 bermanfaat untuk mengenalkan beberapa metode manajemen risiko sistem informasi kepada divisi TI.

3.3. Metode Analisis Risiko *OCTAVE-S*

Dalam penelitian ini, untuk melakukan analisis dan penilaian risiko yang ada, digunakan metode *OCTAVE-,* dimana *OCTAVE-S* sendiri memiliki tiga tahapan utama yaitu:

1) Membuat profil aset beserta ancaman-ancamannya.

Pada fase ini dilakukan evaluasi dari segi aspek organisasi, pada fase ini didefinisikan kriteria evaluasi yang kemudian akan digunakan dalam melakukan evaluasi risiko. Dalam fase ini terdapat dua proses:

a. Identifikasi informasi organisasi

Adapun aktifitas yang dilakukan pada proses ini ada tiga

i. Membuat kriteria dampak evaluasi.
   Dalam penelitian ini akan digunakan empat tabel kriteria risiko: tabel kriteria dampak, tabel kriteria kemungkinan, tabel kriteria pemeringkat risiko, dan tabel kriteria selera risiko.
ii. Mengidentifikasi aset-aset yang dimiliki perusahaan.
   Identifikasi aset dilakukan dengan mengumpulkan informasi aset, berupa jenis, umur, ukuran, lokasi aset, dan tanggal instalasi; penilaian atas kondisi dan kinerja aset termasuk informasi mengenai pengoperasian, riwayat pemeliharaan dan perbaikan.
iii. Melakukan evaluasi terhadap praktek-praktek kemanan organisasi yang sudah berjalan.

2) Membuat profil ancaman terhadap aset-aset perusahaan.

Pada proses ini terdapat empat aktifitas yang mesti dilakukan

i. Menentukan aset-aset perusahaan yang paling penting, artinya jika aset-aset ini terganggu maka akan mengganggu kinerja perusahaan secara luas atau bahkan lebih buruk lagi.
ii. Mengidentifikasi pengamanan yang dilakukan terhadap aset-aset penting tersebut.
iii. Mengidentifikasi ancaman-ancaman yang dapat mengganggu aset-aset penting perusahaan.
iv. Menganalisa teknologi terkait dengan proses yang berjalan selama ini.

2) Mengidentifikasi kelemahan-kelemahan infrastruktur

Pada tahap ini dilanjutkan dengan meneliti hingga sejauh mana setiap orang berpartisipasi untuk bertanggung jawab terhadap praktek-praktek keamanan proses teknologi informasi.

Pada fase ini terdapat satu proses yang harus dilakukan yaitu meneliti infrastruktur komputasi yang berhubungan erat dengan aset-aset penting perusahaan.

Proses tersebut memiliki dua aktifitas yakni:

a. Memeriksa jalur akses yang menuju kepada aset-aset penting perusahaan.
b. Menganalisa teknologi yang berperan untuk mengakses aset-aset penting perusahaan tersebut.

3) Membuat rancangan strategi keamanan

Pada fase ini yang merupakan fase terakhir dalam metode *OCTAVE-S*, dilakukan identifikasi risiko-risiko yang mungkin muncul dan dapat membahayakan aset-aset penting perusahaan, serta memutuskan hal-hal yang harus dilakukan untuk melindungi aset tersebut.

Dari hasil analisis informas yang telah dilakukan sebelumnya maka dapat dibuat strategi perlindungan terhadap aset-aset tersebut, membuat perencanaan mitigasi risiko.

Dalam fase ini terdapat dua proses:

a. Identifikasi dan analisis risiko, dan dalam proses ini terdapat tiga aktifitas yang harus dilakukan
   i. Mengevaluasi dampak dari ancaman.
   ii. Membuat kriteria evaluasi kemungkinan-kemungkinan.
   iii. Mengevaluasi kemungkinan-kemungkinan dari setiap ancaman-ancaman yang dapat muncul.
b. Membuat strategi pengendalian dan rencana mitigasi, pada proses ini terdapat lima aktifitas yang harus dilakukan yakni:
   i. Menggambarkan strategi pengendalian risiko yang telah berjalan sebelumnya.
   ii. Menentukan pendekatan mitigasi risiko yang hendak digunakan.
   iii. Membangun perencanaan mitigasi risiko.
   iv. Mengidentifikasi perubahan terhadap strategi pengendalian.
   v. Mengidentifikasi langkah-langkah pengembangan selanjutnya.

3.4. Metode Pengendalian ISO/EIC 27001:2005

Dari hasil analisis risiko yang didapatkan sebelumnya, dengan menggunakan metode *OCTAVE-S*, dengan memanfaatkan standar ISO/EIC 27001:2005, dimana memiliki pengendalian yang sudah dirumuskan, pada standar pengendalian ISO/EIC 27001:2005 terdapat 11 klausul yakni:

a. Kebijakan keamanan.
b. Pengelolaan keamanan informasi.
c. Manajemen aset.
d. Keamanan sumber daya manusia.
e. Keamanan fisik dan lingkungan.
f. Manajemen komunikasi dan operasional.
g. Pengontrolan akses.
h. Akuisisi, pengembangan, dan perawatan sistem informasi.
i. Manajemen insiden kemanan informasi.
j. Manajemen kelangsungan bisnis.
k. Pemenuhan.

Kesebelas klausul ini memiliki 142 standar pengendalian detail yang akan dipilih, dan digunakan sebagai acuan untuk menetapkan pengendalian yang sesuai dengan kebutuhan perusahaan disesuaikan dengan penilaian risiko sebelumnya.

Hasil akhir dari tahap ini akan mengeluarkan rekomendasi manajemen risiko terhadap ancaman-ancaman yang terdapat di perusahaan PT. Aldira Berkah Abadi Makmur.

4. HASIL DAN PEMBAHASAN

4.4 Pelaksanaan Penilaian Risiko Sistem Informasi Menggunakan Metode OCTAVE-S

4.4.1 Tahap 1-Membangun aset berbasis profil ancaman.

4.4.1.1 Membuat kriteria dampak risiko (Step 1)

Tabel 1. Dampak Risiko-Reputasi dan kepercayaan pelanggan

		LOW IMPACT	MEDIUM IMPACT	HIGH IMPACT
Reputasi dan kepercayaan pelanggan	Reputasi	Reputasi hampir tidak terpengaruh, membutuhkan sedikit atau tidak ada usaha yang diperlukan untuk mengembalikan reputasi.	Reputasi terkena dampak buruk, dan dibutuhkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
	Kehilangan Pelanggan	Pengurangan pelanggan kurang dari 5% akibat kehilangan kepercayaan pelanggan	Pengurangan pelanggan antara 5% hingga 15% akibat kehilangan kepercayaan pelanggan.	Pengurangan pelanggan lebih dari 15% akibat kehilangan kepercayaan pelanggan

Tabel 2. Dampak Risiko- Keuangan

		LOW IMPACT	MEDIUM IMPACT	HIGH IMPACT
Keuangan	Biaya operasional	Biaya meningkat kurang dari 2% di bulan berjalan dibandingkan bulan sebelumnya.	Biaya meningkat antara 2%-15% di bulan berjalan dibandingkan bulan sebelumnya.	Biaya meningkat lebih dari 15% di bulan berjalan dibandingkan bulan sebelumnya.
	Keuntungan Perusahaan	Menurunnya *income* perusahaan kurang dari 5% dibulan berjalan.	Menurunnya pemasukan perusahaan antara dari 5%-20% dibulan berjalan.	Menurunnya pemasukan perusahaan lebih dari 20% dibulan berjalan.
	Kerugian Secara Langsung	Kerugian langsung kurang dari Rp15.000.000,-	Kerugian langsung mencapai angka Rp15.000.000,- hingga Rp100.000.000,-	Kerugian langsung mencapai angka lebih dari Rp100.000.000,-

Tabel 3. Dampak risiko -Produktivitas

		LOW IMPACT	MEDIUM IMPACT	HIGH IMPACT
Produktivitas	Waktu kerja Karyawan	Waktu kerja karyawan meningkat kurang dari 10% dalam kurun waktu 2 hari.	Waktu kerja karyawan meningkat antara 10%-30 % dalam kurun waktu 2 hari.	Waktu kerja karyawan meningkat lebih dari 30 % dalam kurun waktu 2 hari.
	Kuantitas Proses Dokumen	Kuantitas proses dokumen yang dilakukan karyawan menurun kurang dari 10% dalam waktu 2 hari.	Kuantitas proses dokumen yang dilakukan karyawan menurun antara 10% hingga 30 % dalam waktu 2 hari.	Kuantitas proses dokumen yang dilakukan karyawan menurun antara lebih dari 30 % dalam waktu 2 hari.

Tabel 4. Dampak risiko-Denda dan Penalti

		LOW IMPACT	MEDIUM IMPACT	HIGH IMPACT
Denda dan Penalti	Denda	Denda kurang dari Rp.15.000.000,-	Denda antara Rp.15.000.000,- hingga Rp.75.000.000,-	Denda lebih dari Rp.75.000.000,-
	Tuntutan Hukum	Tuntutan kecil atau tuntutan dengan nilai kurang dari Rp.15.000.000,- akan dikenakan kepada perusahaan.	Tuntutan dengan nilai antara Rp.15.000.000,- hingga Rp.75.000.000,- akan dikenakan kepada perusahaan.	Tuntutan dengan nilai lebih dari Rp.75.000.000,- akan dikenakan kepada perusahaan.
	Investigasi	Tidak adanya pemeriksaan dari pemerintah atau organisasi investigasi lainnya.	Pemerintah atau organisasi investigasi lainnya akan meminta catatan-catatan yang terkait dengan tuntutan.	Pemerintah atau organisasi investigasi lainnya akan memulai penyelidikan yang lebih mendalam terhadap praktek bisnis perusahaan.

4.4.1.2 Mengidentifikasi aset-aset informasi perusahaan (Step 2)

Pada aktivitas yang kedua ini, dilakukan identifikasi aset-aset informasi yang dimiliki oleh PT Aldira Berkah Abadi Makmur, dimana dalam menentukan aset informasi tersebut dibagi dalam dua kategori aset, kategori yang pertama adalah aset-aset yang berkaitan dengan informasi, sistem, dan aplikasi-aplikasi yang dimiliki oleh PT Aldira Berkah Abadi Makmur, adapun kategori yang kedua adalah *people*(karyawan), kategori *people* dilihat dari seberapa spesialnya karyawan tersebut hingga tidak dapat digantikan, dimana karyawan tersebut menjadi aset perusahaan dan akan terjadi masalah seandainya karyawan tersebut tidak ada.

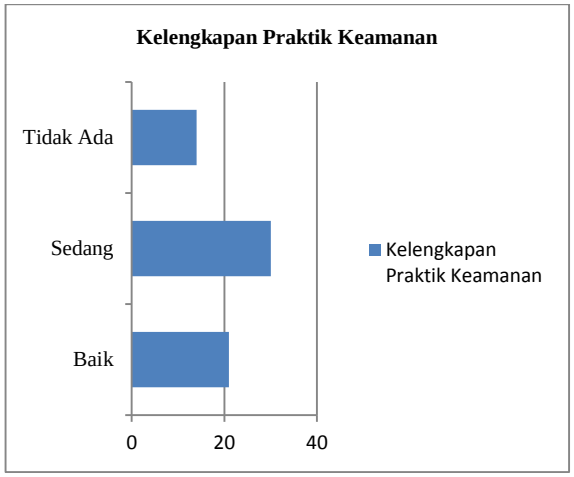
4.4.1.3 Mengevaluasi keamanan perusahaan yang telah berjalan (Step 3-4).

Dalam mengevaluasi keamanan perusahaan yang telah berjalan di PT Aldira Berkah Abadi Makmur digunakanlah 15 praktek keamanan yang terdapat dalam OCTAVE-S adapun ke 15 praktek kemanan tersebut adalah:

1. Kesadaran Keamanan dan Pelatihan
2. Strategi Keamanan
3. Manajemen Keamanan
4. Kebijakan Keamanan dan Peraturan
5. Manajemen Keamanan dan Kolaboratif
6. Rencana Kemungkinan atau Pemulihan dari Bencana
7. Pengendalian Akses Fisik

8. Pemantaun dan Audit Keamanan Fisik
9. Sistem Manajemen Jaringan.
10. Pemantauan dan Keamanan TI
11. Pengesahan dan Otorisasi
12. Manajemen Kerentanan
13. Enkripsi
14. Desain dan Arsitektur
15. Manajemen Insiden

Secara keseluruhan maka kelengkapan dari 15 praktik kemanan yang dianjurkan OCTAVE didapatkan hasil seperti gambar tertera dibawah ini.



Gambar 7. Kelengkapan praktik kemanan keseluruhan

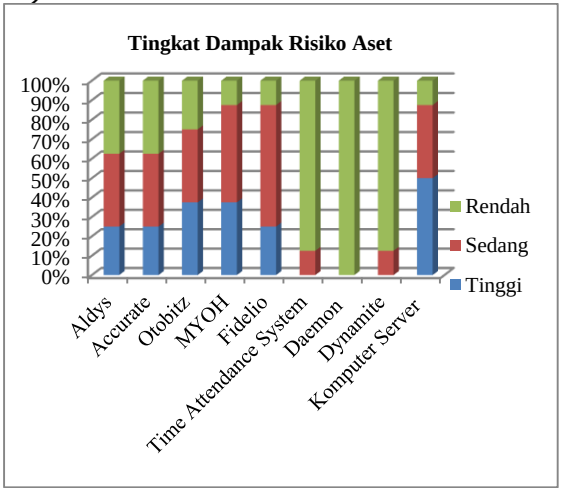
4.4.1.4 Menentukan aset-aset yang paling penting (Steps 5-9).

Dari hasil wawancara dan hasil observasi yang dilakukan di perusahaan PT Aldira Berkah Abadi Makmur didapatkanlah aset-aset penting yang dimiliki perusahaan, dimana tanpa adanya aset ini perusahaan akan mengalami kendala dalam kegiatan proses bisnis yang dijalankannya, yang dapat menimbulkan kerugian bagi perusahaan. Adapun detail dari aset-aset penting perusahaan digambarkan pada tabel 26 dibawah.

Tabel 5. Aset-aset penting PT Aldira Berkah Abadi Makmur

No	Aset Penting	Keterangan
1	Aldys	Aldys sangat diperlukan untuk melakukan pencatatan permintaan barang, penerimaan barang dan proyek-proyek yang dijalankan oleh perusahaan holding.
2	Accurate	Informasi keuangan seluruh perusahaan disimpan dengan menggunakan aplikasi Accurate.
3	Otobitz	Transaksi bisnis PT RHYSS tersimpan dengan menggunakan aplikasi Otobitz.
4	MYOH	Transaksi bisnis dari front office seperti reservasi kamar, back office keuangan dan inventory serta transaksi income dari food and beverages Apartemen Shinju disimpan dengan mengakses aplikasi MYOH.
5	Fidelio	Karyawan Hotel Harrads menyimpan seluruh transaksi hotel dengan menggunakan aplikasi Fidelio.
6	Time Attendance System	Karyawan yang berada di holding melakukan absensi dengan menggunakan fingerprint yang disimpan melalui aplikasi ini.
7	Daemon	Daemon digunakan untuk memenej email perusahaan untuk seluruh karyawan.
8	Dynamite	Dynamite digunakan untuk memenej data telepon perusahaan (PABX)
9	Komputer Server	Komputer server menyimpan data-data backup perusahaan, dan database dari aplikasi aldys.

4.4.1.5 Mengidentifikasi kebutuhan keamanan aset-aset penting (Steps 10-11)



Gambar 8. Tingkat Dampak Risiko Aset ABAM

4.4.1.6 Mengidentifikasi ancaman-ancaman terhadap aset-aset penting (Steps 12-16)

Tahap ini merupakan tahap dimana tim melakukan identifikasi ancaman-ancaman yang mungkin terjadi pada perusahaan, dari hasil wawancara terhadap beberapa staf termasuk juga staf TI perusahaan, didapatkanlah ancaman-ancaman yang mungkin terjadi dan bagaimana histori ancaman yang pernah terjadi pada perusahaan PT Aldira Berkah Abadi Makmur, maka dihasilkan seperti dibawah ini terhadap lima aset penting perusahaan.

4.4.2 Melakukan identifikasi terhadap kerentanan infrastruktur.

4.4.2.1 Memeriksa jalur akses (Steps 17-18).

Tahap ini merupakan tahap untuk mengetahui bagaimana seseorang dapat mengakses aset-aset penting yang dimiliki oleh perusahaan PT Aldira Berkah Abadi Makmur.

Tabel 6. *System of interest, access points* dan *system access by people*

System of Interest	*Intermediate Access Points*	*System Access by People*
Kelas komponen mana yang dibawah ini yang merupakan bagian dari *system of interest*	Kelas komponen mana yang dibawah ini yang digunakan untuk mengirimkan informasi?	Dari mana user atau penyusup dapat mengakses *system of interest*
☑ *Server*	☑ *Internal Networks*	☑ PC Internal
☐ *Internal Network*	☐ *External Network*	☑ Laptop
☑ *On-Site Workstations Purchasing, GA, Interior, Finance, Accounting*		☐ PDA ☐ PC Eksternal

Tabel 7. Penyimpanan data dan komponen lain terkait *system of interest*

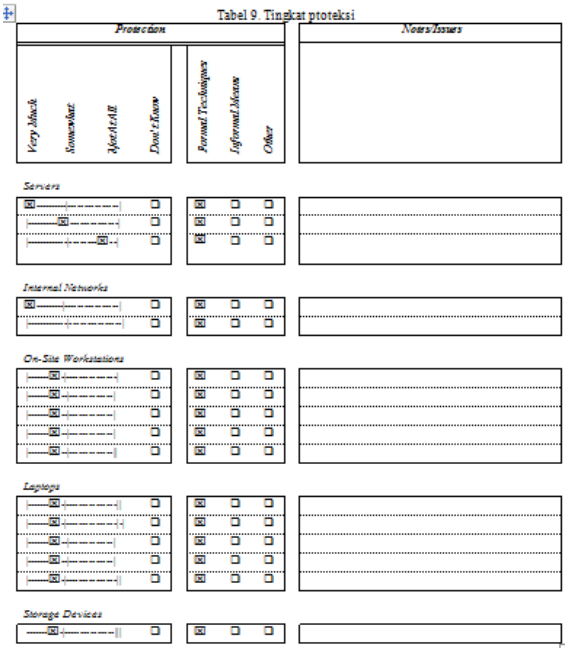
Data Storage Location	*Other Systems and Components*
Kelas komponen mana yang dibawah ini yang merupakan informasi dari *system of interest* disimpan untuk tujuan cadangan?	Sistem apapun yang menggunakan kelas komponen yang sama dengan *system of interest*
☑ Tempat Penyimpanan *Local Backup*	☑ Otobitz
	☑ MYOH
	☑ Aldys
	☑ System lain.

4.4.2.2 Menganalisa proses yang terkait dengan teknologi (Steps 19-21).

Tabel 8 Aset paling penting dan tanggung jawab

Class — *Which classes of components are related to one or more critical assets?*	*Critical Assets* — *Which critical assets are related to each class?*					*Responsibility* — *Who is responsible for maintaining and securing each class of component?*
(Document any relevant subclasses or specific examples when appropriate.)	1. Aldys	2. Accurate	3. MYOH	4. Otobitz	5. Komp Server	
Servers						
Server A	✓			✓	✓	Staf TI Jaringan
Server B		✓				Staf TI Jaringan
Server C			✓			Staf TI Jaringan
Internal Networks						
Semua Aset	✓	✓	✓	✓	✓	Staf TI Jaringan
On-Site Workstations						
Div GA, Purchasing, Interior.	✓				✓	Staf TI *System & Hardware*
Div *Finance* Acc		✓			✓	Staf TI *System & Hardware*
User PT RHYS	✓			✓	✓	Staf TI *System & Hardware*
User PT Shinjo			✓			Staf TI *System & Hardware*
User PT Andi Arta		✓			✓	Staf TI *System & Hardware*
Laptop						
Manajer, GM, Direktur Finance		✓			✓	Staf TI *System & Hardware*
Manajer, Direktur Shinjo			✓			Staf TI *System & Hardware*
Manajer, Direktur Interior	✓				✓	Staf TI *System & Hardware*
Manajer, GM, Direktur RHYS				✓	✓	Staf TI *System & Hardware*
Manajer, Direktur Andi Arta		✓			✓	Staf TI *System & Hardware*
Storage Devices						
Local Back-up	✓	✓	✓	✓	✓	Staf TI *System & Hardware*

Tabel 9. Tingkat ptoteksi



4.4.3 Membangun perencanaan dan strategi keamanan.

4.4.3.1 Evaluasi dampak ancaman (Step 22).

Dari proses identifikasi dan analisis risiko diperoleh hasil dampak dari ancaman yang terjadi, dampak ancaman pada aset penting PT. Aldira Berkah Abadi Makmur dapat terjadi melalui akses jaringan dan akses fisik. Dampak ancaman pada aset penting PT. Aldira Berkah Abadi Makmur melalui akses jaringan yang dilakukan oleh karyawan terhadap PT. Aldira Berkah Abadi Makmur dibagi menjadi 2 kriteria yaitu:

1. Dampak ancaman pada aset penting melalui akses jaringan yang dilakukan oleh karyawan PT. Aldira Berkah Abadi Makmur secara tidak sengaja

Tabel 10. Pofil risiko secara tidak sengaja oleh pihak internal.

Aset Penting	Tipe Dampak	Penyingkapan	Modifikasi	Data Hilang	Interupsi
Aldys	Reputasi	Rendah	Rendah	Sedang	Sedang
	Financial	Rendah	Rendah	Sedang	Sedang
	Produktifitas	Sedang	Sedang	Tinggi	Tinggi
	Denda	Sedang	Rendah	Sedang	Rendah
Accurate	Reputasi	Sedang	Sedang	Sedang	Sedang
	Financial	Sedang	Sedang	Sedang	Sedang
	Produktifitas	Rendah	Sedang	Tinggi	Sedang
	Denda	Sedang	Sedang	Sedang	Sedang
Otobitz	Reputasi	Rendah	Rendah	Rendah	Rendah
	Financial	Rendah	Rendah	Sedang	Rendah
	Produktifitas	Sedang	Sedang	Tinggi	Rendah
	Denda	Sedang	Sedang	Tinggi	Rendah
MYOH	Reputasi	Rendah	Rendah	Rendah	Rendah
	Financial	Rendah	Rendah	Sedang	Rendah
	Produktifitas	Sedang	Sedang	Tinggi	Rendah
	Denda	Sedang	Sedang	Tinggi	Rendah
Komputer server	Reputasi	Rendah	Rendah	Rendah	Rendah
	Financial	Rendah	Rendah	Sedang	Sedang
	Produktifitas	Sedang	Sedang	Tinggi	Sedang
	Denda	Sedang	Sedang	Tinggi	Rendah

2. Dampak ancaman pada aset penting melalui akses jaringan yang dilakukan oleh karyawan PT. Aldira Berkah Abadi Makmur secara sengaja.

Tabel 11. Pofil risiko secara sengaja oleh pihak internal.

Aset Penting	Tipe Dampak	Penyingkapan	Modifikasi	Data Hilang	Interupsi
Aldys	Reputasi	Sedang	Sedang	Sedang	Sedang
	Financial	Sedang	Sedang	Sedang	Sedang
	Produktifitas	Rendah	Sedang	Tinggi	Tinggi
	Denda	Sedang	Sedang	Sedang	Sedang
Accurate	Reputasi	Sedang	Sedang	Sedang	Sedang
	Financial	Sedang	Sedang	Sedang	Sedang
	Produktifitas	Rendah	Sedang	Tinggi	Tinggi
	Denda	Sedang	Sedang	Sedang	Sedang
Otobitz	Reputasi	Sedang	Sedang	Sedang	Rendah
	Financial	Sedang	Sedang	Sedang	Rendah
	Produktifitas	Rendah	Sedang	Tinggi	Sedang
	Denda	Rendah	Rendah	Sedang	Sedang
MYOH	Reputasi	Sedang	Sedang	Rendah	Rendah
	Financial	Sedang	Sedang	Sedang	Sedang
	Produktifitas	Rendah	Sedang	Tinggi	Tinggi
	Denda	Rendah	Rendah	Sedang	Sedang
Komputer server	Reputasi	Sedang	Rendah	Rendah	Rendah
	Financial	Sedang	Sedang	Sedang	Rendah
	Produktifitas	Rendah	Sedang	Tinggi	Tinggi
	Denda	Rendah	Rendah	Sedang	Rendah

4.4.3.2 Membangun kriteria evaluasi (Step 23).

Tabel 12. Kriteria frekuensi

Kriteria Berdasarkan Frekuensi			
	Tinggi	Sedang	Rendah
Waktu antar peristiwa	> 9 kali dalam 1 Tahun	<9 dan>4 kali dalam 1 Tahun	< 4 kali dalam 1 Tahun
Frekuensi tahunan	>9	<9 dan>4	<4

4.4.3.3 Mengevaluasi kemungkinan ancaman-ancaman yang dapat muncul (Step 24).

Dari kertas kerja hasil wawancara dan kuesioner maka didapat hasil peluang dari ancaman sebagai berikut:

1. *Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak dalam perusahaan melalui akses jaringan dan fisik.*
   Untuk peluang terjadinya ancaman yang secara tidak sengaja dilakukan oleh pihak internal, yang memiliki kemungkinan paling tinggi ada pada kategori modifikasi dan data hilang pada aplikasi aldys, accurate, dan MYOH karena pada ketiga aplikasi inilah kejadian ini sering terjadi adapun untuk aset yang lain kemungkinan terjadinya ancaman-ancaman rendah karena jarang terjadi.
2. *Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak dalam perusahaan melalui akses jaringan dan fisik.*
   Untuk peluang terjadinya ancaman yang secara sengaja dilakukan oleh pihak internal, yang memiliki kemungkinan paling tinggi ada pada kategori penyingkapan, modifikasi dan data hilang pada aplikasi otobitz, accurate, dan MYOH karena pada ketiga aplikasi inilah kejadian ini sering terjadi, kasus yang paling sering terjadi adalah, dimana karyawan dengan sengaja melakukan modifikasi dengan memanipulasi pemasukan, dan karyawan leluasa dalam mengakses aset sistem informasi perusahaan, adapun untuk aset yang lain kemungkinan terjadinya ancaman-ancaman rendah karena jarang terjadi.
3. Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan dan fisik.
   Berdasarkan histori perusahaan peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan sangat rendah, dan belum pernah terjadi karena aset sistem informasi tidak bisa diakses dari luar perusahaan, namun peluang paling tinggi ada pada aset MYOH dengan tingkat keyakinan sedang, karena akses jaringan luar dengan jaringan internal tidak diproteksi dengan keamanan yang baik.
4. *Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan dan fisik.*
   Kemungkinan terjadinya ancaman yang secara sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan yang paling tinggi adalah ancaman penyingkapan, pada aset MYOH dan *accurate* dengan tingkat keyakinan sedang, karena kedua aset ini tidak terproteksi dan terawat dengan baik.
5. *Peluang terjadinya ancaman lain-lain.*
   Peluang terjadingan ancaman yang paling tinggi adalah pada ancaman kerusakan sistem, permasalahan pada hardware, dan malicious code seperti virus dan sebagainya, termasuk pada semua aset paling penting baik itu aldys, accurate, MYOH, dan otobitz dengan tingkat keyakinan tinggi, sedangkan untuk asset komputer server lebih cenderung kepada ancaman permasalahan pada hardware, dan malicious code dengan tingkat keyakinan tinggi. Sedangkan yang lainnya tergolong sedang.

4.4.3.4 Strategi proteksi yang sudah ada (Step 25).

Dari penelitian yang dilakukan di perusahaan dengan menggunakan pendekatan

OCTAVE-S, dapat ditemukan beberapa risiko dari penerapan teknologi informasi yang berkaitan dengan praktik keamanan yang ada pada perusahaan. Risiko–risiko yang ditemukan ada 11 hal yaitu:

1. Kesadaran keamanan dan pelatihan.
2. Strategi kemanan.
3. Manajemen kemanan.
4. Kebijakan kemanan dan peraturan.
5. Rencana kemungkinan atau pemulihan dari bencana
6. Pengendalian akses fisik.
7. Pemantauan audit dan kemanan fisik.
8. Sistem dan manajemen jaringan
9. Pengesahan dan otorisasi.
10. Enkripsi.
11. Desain dan arsitektur kemanan.

4.4.3.5 Menentukan pendekatan mitigasi (Steps 26-27)

Sebelum melangkah pada tahap berikutnya dimana pada tahap 28 merupakan langkah dalam pembuatan rencana mitigasi terhadap risiko-risiko yang ditemukan, maka hasil pekerjaan yang dilakukan dari tahap 1 hingga tahap 25 dikonsultasikan bersama untuk menentukan pendekatan mitigasi yang harus dilakukan, risiko apa yang perlu dimitigasi dan risiko apa yang tidak perlu dimitigasi

Berdasarkan hasil kesepakatan bersama yang dirujuk dari kertas kerja yang didapat dari hasil wawancara, kuesioner dan temuan dari langkah demi langkah yang telah dilakukan, maka dihasilkan kesepakatan bahwa pendekatan mitigasi dilakukan pada ancaman yang mempunyai motif disengaja pada internal maupun eksternal perusahaan melalui akses jaringan dan fisik.

4.4.3.6 Membuat rencana mitigasi risiko (Step 28)

Pada tahap ini dibuatnya rencana mitigasi risiko dengan mengambil kontrol-kontrol pengendalian yang terdapat pada ISO 27001:2005 sebagaimana terdapat pada tabel

Tabel 44. Rencana mitigasi risiko

ANCAMAN	ASPEK	PENGENDALIAN ISO 27001:2005	PERENCANAAN	IMPLEMENTASI	RENCANA EVALUASI
1. Organisasi tidak menjadikan pelatihan kesadaran kemanan kepada staf baru sebagai kegiatan yang harus dilakukan. 2. Kurangnya dokumentasi akan kebijakan kemanan informasi perusahaan.	Kesadaran kemanan dan pelatihan.	1. Semua karyawan organisasi dan, bila relevan, kontraktor dan pengguna pihak ketiga harus menerima pelatihan kesadaran yang tepat dan update reguler mengenai prosedur dan kebijakan organisasi, sebagai bagian dari fungsi pekerjaan mereka.(A.8.2.2) 2. Prosedur operasional harus didokumentasikan, dipertahankan, dan tersedia untuk semua pengguna yang membutuhkannya. (A.10.1.1)	1. Pembuatan peraturan dan sangsi, yang harus ditandatangani oleh manajemen tertinggi. 2. Sosialisasi peraturan yang telah disetujui. 3. Melakukan pelatihan akan kemanan sistem informasi dan penggunaan *pasword*.	Diberlakukan setelah seluruh manajemen menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	Periodik 2 x dalam satu tahun
3. Karyawan kurang memahami tanggung jawab dan kebijakan keamanan. 4. Karyawan masih suka berbagi *username* dan *password*.		3. Peran keamanan dan tanggung jawab karyawan, kontraktor dan pengguna pihak ketiga harus ditetapkan dan didokumentasikan sesuai dengan kebijakan keamanan informasi organisasi. (A.8.1.1). 4. Manajemen harus mensyaratkan pegawai, kontraktor dan pengguna pihak ketiga untuk menerapkan keamanan sesuai dengan kebijakan dan prosedur organisasi. (A.8.2.1) 5. Harus ada proses pendisiplinan formal untuk karyawan yang telah melakukan pelanggaran keamanan. (A.8.2.3) 6. Alokasi password harus dikendalikan melalui proses manajemen formal. (A.11.2.3). 7. Manajemen harus meninjau hak akses pengguna secara teratur yang menggunakan proses formal. 8. Pengguna wajib untuk mengikuti praktik keamanan yang baik dalam pemilihan dan penggunaan password.			
5. Perusahaan belum pernah melakukan uji coba terhadap rencana kontinuitas bisnis dan disaster recovery plan. 6. Akses fisik dan elektronik kedalam informasi penting tidak disertakan kedalam DRP dan BCP. 7. Tidak adanya pelatihan yang menyertakan DRP dan BCP perusahaan kepada karyawan yang ada.	Rencana kemungkinan atau pemulihan dari bencana	9. Perlu dibuatkan dan diterapkan SOP untuk menjaga kelangsungan bisnis di seluruh organisasi yang membahas persyaratan kemanan informasi yang dibutuhkan untuk kelangsungan bisnis organisasi. (A.14.1.1) 10. Peristiwa yang bisa menyebabkan gangguan terhadap proses bisnis harus diidentifikasi, bersama dengan probabilitas dan dampak dari gangguan tersebut dan konsekuensinya terhadap keamanan informasi. (A.14.1.2) 11. Rencana harus dikembangkan dan diimplementasikan untuk mempertahankan atau mengembalikan operasi dan memastikan ketersediaan informasi pada tingkat yang diperlukan dan dalam skala waktu yang dibutuhkan setelah interupsi, atau kegagalan, proses bisnis penting. (A.14.1.3) 12. Sebuah kerangka tunggal dari rencana kesinambungan bisnis	1. Pembuatan peraturan dan sangsi, yang harus ditandatangani oleh manajemen tertinggi. 2. Sosialisasi peraturan yang telah disetujui. 3. Melakukan pelatihan akan rencana DRP dan BCP yang telah ditetapkan perusahaan.	Diberlakukan setelah seluruh manajemen menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	Periodik 2 x dalam satu tahun
		harus dipelihara untuk memastikan semua rencana yang konsisten, untuk secara konsisten menangani kebutuhan keamanan informasi, dan untuk mengidentifikasi prioritas untuk pengujian dan pemeliharaan. (A.14.1.4) 13. Rencana kontinuitas bisnis harus diuji dan diperbarui secara teratur untuk memastikan bahwa rencana yang dibuat selalu *up to date* dan efektif. (A.14.1.5) 14. Perlindungan fisik terhadap kerusakan akibat kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil, dan bentuk-bentuk lain dan bencana alam atau buatan manusia harus dirancang dan diterapkan. (A.9.1.4)			
8. Organisasi tidak mengevaluasi untuk memperbaharui dokumen,	Kebijakan kemanan dan peraturan.	15. Sebuah dokumen kebijakan keamanan informasi harus disetujui oleh manajemen, dan dipublikasikan dan dikomunikasikan kepada	1. Pembuatan peraturan dan sangsi, yang harus ditandatangani oleh manajemen tertinggi.		
kebijakan. 9. Kurangnya dokumentasi proses untuk melakukan evaluasi dan memastikan kepatuhan terhadap kebijakan keamanan, hukum-hukum yang dipakai dan aturan-aturan, dan kebutuhan penjaminan.		seluruh karyawan dan pihak eksternal. (A.8.2.3) 16. Prosedur operasional harus didokumentasikan, dipertahankan, dan tersedia untuk semua pengguna yang membutuhkannya. (A.10.1.1) 17. Kebijakan keamanan informasi harus ditinjau pada selang waktu terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan, dan efektifitas. (A.5.1.2)	2. Sosialisasi peraturan yang telah disetujui.		
10. Tidak adanya dokumentasi dan rencana uji keamanaan untuk menjaga sistem dan jaringan. 11. Peralatan dan mekanisme untuk keamanan sistem dan jaringan administrasi yang digunakan, jarang	Manajemen sistem dan jaringan.	18. Prosedur operasional harus didokumentasikan, dipertahankan, dan tersedia untuk semua pengguna yang membutuhkannya. (A.10.1.1) 19. Jaringan harus dibelola dan dikendalikan secara memadai, untuk dilindungi dari ancaman, dan untuk menjaga keamanan untuk sistem dan aplikasi yang menggunakan jaringan, termasuk proses penguinan	1. Pembuatan peraturan dan sangsi, yang harus ditandatangai oleh manajemen tertinggi. 2. Pembuatan SOP untuk setiap sub divisi TI secara lengkap. 3. Sosialisasi peraturan yang telah disetujui.		
ditinjau secara rutin dan diperbarui atau diganti waktu sudah tidak layak digunakan.		informasi. (A.10.6.1) 20. Fitur keamanan, tingkat pelayanan, dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan termasuk dalam setiap perjanjian layanan jaringan, apakah layanan ini disediakan in-house maupun outsourcing. (A.10.6.2)			

Tabel 14. Kebijakan mitigasi risiko

KEBIJAKAN MITIGASI	ALASAN	PENANGGUNG JAWAB	PENDUKUNG
Mensosialisasikan kebijakan melalui papan pengumuman, email, dan forum Aldira.	Agar seluruh karyawan memahami tentang adanya peraturan yang akan ditetapkan beserta sanksi bagi yang melanggar peraturan tersebut	Manajer TI, Manajer HRD	Komitmen dan dukungan staf hingga direksi(pimpinan)

4.4.3.7 Identifikasi langkah selanjutnya (Step 29-30).

Tim mengidentifikasi beberapa kebutuhan yang diperlukan untuk implementasi hasil dari OCTAVE-S.

Manajemen risiko akan berjalan dengan sukses apabila:

- Dukungan secara penuh dari management IT untuk menjalankan standar prosedur.
- Kesadaran dan kerjasama dari seluruh staff, untuk mengikuti prosedur managemen risiko.
- Kompetensi dari risk assessment team yang baik, dimana team tersebut memiliki pengalaman untuk mengaplikasikan metodologi terhadap sistem secara tepat, dan tentu memberikan perlindungan dengan efektivitas biaya untuk memenuhi kebutuhan perusahaan.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil penelitian dan analisis yang telah dilakukan maka dapat diambil beberapa kesimpulan dari penggunaan OCTAVE-S sebagai acuan dasar melakukan evaluasi risiko pada PT. ALDIRA BERKAH ABADI MAKMUR serta ISO 27001:2005 yang dijadikan sebagai pengendalian atas ancaman-ancaman dari aspek keamanan sistem informasi yang dipilih:

1. Dengan melakukan evaluasi risiko dengan menggunakan OCTAVE-S maka perusahaan dapat memetakan risiko dan kelemahan sistem informasi perusahaan.
2. Dengan dilakukannya manajemen risiko sistem informasi, PT. ALDIRA BERKAH ABADI MAKMUR dapat mengetahui seberapa besar dampak risiko, ancaman serta kelemahan yang muncul terhadap kelangsungan bisnis perusahaan.
3. PT. ALDIRA BERKAH ABADI MAKMUR kurang dalam melakukan dokumentasi-dokumentasi, khususnya dalam prosedur-prosedur operasional divisi TI, serta dokumentasi yang berkenaan dengan penilaian terhadap asset penting perusahaan.
4. Dari hasil pengukuran *risk exposure* dari hasil evaluasi, dapat diketahui bahwa manajemen risiko berada pada posisi SEDANG, artinya perusahaan tidak mengalami risiko yang dapat menghentikan/merusak sistem informasi perusahaan yang berdampak pada berhentinya proses bisnis perusahaan jika terjadi risiko tersebut, namun risiko dan kelemahan pada perusahaan dapat berdampak pada menurunnya kinerja perusahaan jika tidak ditangani dengan segera.
5. Dengan menggunakan pengendalian yang ada pada ISO 27001:2005 dapat membantu perusahaan dalam melakukan persiapan saat akan mengimplementasikan standar ISO khususnya bagi divisi teknologi informasi perusahaan.

5.2 Saran

Dalam evaluasi sistem informasi manajemen risiko menggunakan OCTAVE-S ini, hanya memberikan informasi tentang risiko dan kelemahan pada perusahaan dan masukan untuk penanganan risiko dan kelemahan dibatasi hanya pada risiko tingkat *exposure* > Sedang. Oleh karena itu saya menyampaikan saran kepada pihak manajemen PT. ALDIRA BERKAH ABADI MAKMUR agar:

1. Melengkapi praktik keamanan yang disarankan OCTAVE setidaknya yang

dijadikan prioritas dari 15 praktik keamanan.
2. Membuat prosedur mengenai praktik-praktik keamanan secara lebih formal untuk menjalankan kemanan TI secara konsisten.
3. Implementasikan SOP manajemen risiko dalam prosedur sekecil apapun karena risiko dan kelemahan selalu berawal dari sebuah kesalahan kecil yang menimbulkan lubang pada keamanan sistem informasi.
4. Menyediakan pelatihan-pelatihan kesadaran keamanan pada seluruh karyawan PT. ALDIRA BERKAH ABADI MAKMUR. Hal ini penting agar karyawan mengerti bagaimana menjaga keamanan yang akan meminimalkan risiko.

Secara berkala melakukan audit keamanan sistem informasi untuk mengetahui kebutuhan dan kelemahan keamanan sistem informasi karena terus berkembangnya teknologi menyebabkan jenis serangan/risiko akan semakin berkembang.

DAFTAR PUSTAKA

Albert, C., & Dorofee, A. (2003). *Managing Information Security Risks: The OCTAVESM Approach.* USA: Addison Wesley.

Alberts, C. J., & Dorofee J, A. (2001). *OCTAVESM Method Implementation Guide Version 2.0.* USA: Carnegie Mellon University.

Ambarriani, S. (2000). *Manajemen Biaya.* Jakarta: Salemba Empat.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly* , 413-438.

Barlette, Y. (2006). Les comportements sécuritares des acteurs dans les systémes d'information des pme. *Université de Montpellier I* .

Bornman, W., & Labuschagne, L. (2004). A COMPARATIVE FRAMEWORK FOR EVALUATING INFORMATION SECURITY RISK MANAGEMENT METHODS. *Standard Bank Academy for Information Technology* .

Brenner, J. (2007). ISO 27001 Risk Management and Compliance. *Risk Management Journal* .

Bringham, E., Gapenski, L., & Daves, P. (1999). *Intermediate Financial Management.* New York: The Dryden Press.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* USA: Carnegie Mellon University.

Coleman, J. (2004). Assessing Information Security Risk in Healthcare Organizations of Different Scale. *Proceedings of the 18th International Congress and Exhibition* (hal. 125-130). Elsevier.

Coleman, J. (2004). Assessing Information Security Risk in Healthcare Organizations of Different Scale. *Proceedings of the 18th International Congress and Exhibition* (hal. 125-130). London: Elsevier.

Education, Audittindo. (2006). *An Introductory Course for Implementing Risk-Based Auditing.* Jakarta: PT Audittindo Arin Prima.

ENISA. (2006). *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools.* USA: ENISA.

Ernst, & Young's. (2008). *Moving beyond compliance Information Security Survey.* USA: Ernst & Young's.

FARAHMAND, F., & NAVATHE, S. B. (2005). A Management Perspective on Risk of Security Threats to Information Systems. *Information Technology and Management* , 203–225.

Humfreys, T. (2005). State-of-the-art information security management system with ISO/IEC 27001:2005. *ISO Management Systems* , 15-18.

ISO, & EIC. (2005). *International Standard, Information Technology-Security Techniques-Information Security Management System-Requirements.* London: British Standard Institution.

Jake Kouns, D. M. (2010). *Information Technology Risk Management in Enterprise Enviroments.* New Jersey: John Wiley & Sons.

Kloman, H. F. (2000). *Risk Management Reports.* USA: Press Inc.

Laudon, K. C., & Traver, C. G. (2003). *E-Commerce, Business, Technology, Society* (2nd Edition ed.). New York: Pearson.

Rokhman, F. (2007). *Perancangan Dan Implementasi Sistem Manajemen Keamanan Informasi Berbasis: Standar ISO/IEC 17799, ISO/IEC 27001, dan Analisis Risiko Metode Octave-S.* Bandung: Institut Teknologi Bandung.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal , IV*, 60-66.

Satti, M. M., Nagrial, M. H., & Garner, B. J. (2002). Framework of Information Security Management System (ISMS) Standards ISO 17799 / BS 7799. *Journal of Management* .

Selim, G. M., & McNamee, D. (1998). *Risk Management: Changing the Internal Auditor's Paradigm.* Sping Florida: Institute Of Internal Auditors Research Foundation.

Shedden, P., Smith, W., Scheepers, R., & Ahmad, A. (2009). Towards a Knowledge Perspective in Information Security Risk Assessments-an Illustrative Case Study. *20th Australasian Conference on Information Systems* (hal. 2-4). Melbourne: Information Security Risk Assessments Press.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* USA: National Institute of Standards and Technology.

Woody, C. (2006). *Applying OCTAVE: Practitioners Report.* Australia: Carnegie Mellon University.

Woody, C. (2005). *OCTAVE in Practice.* Melbourne: Carnegie Mellon University.