BAB 2

LANDASAN TEORI

2.1 Teknologi Informasi

Teknologi informasi merupakan salah satu variabel yang berhubungan dengan penelitian kami. Oleh sebab itu kami membahas beberapa teori yang menjelaskan dan teori yang berhubungan dengan teknologi informasi.

2.1.1 Pengertian Informasi

Menurut McLeod & Schell (2007, p15), informasi adalah data yang telah diproses atau data yang memiliki arti, biasanya informasi menjelaskan sesuatau yang belum diketahui kepada *user*.

Menurut O'Brien (2007, p29), informasi adalah data yang telah diubah menjadi konteks yang berarti dan berguna bagi pemakai akhir tertentu.

Dari definisi-definisi diatas dapat disimpulkan bahwa informasi adalah sekumpulan data yang telah diolah atau diproses sehingga memiliki arti untuk diketahui atau digunakan oleh pengguna tertentu.

2.1.2 Pengertian Sistem Informasi

Menurut O'Brien (2007, p45), sistem informasi adalah gabungan yang terorganisasi dari manusia, perangkat lunak, perangkat keras, jaringan komunikasi, dan sumber daya data dalam mengumpulkan, mengubah, dan menyebarkan informasi dalam organisasi.

Menurut Gondodiyoto (2007, p112), menyatakan bahwa sistem informasi masih dapat didefinisikan sebagai kumpulan elemen-elemen atau sumber daya dan jaringan prosedur yang saling berkaitan secara terpadu, terintegrasi dalam suatu hubungan hierarki tertentu, dan bertujuan untuk mengolah data menjadi informasi.

Dari kedua definisi tersebut dapat disimpulkan bahwa sistem informasi adalah sekumpulan data olahan yang terintegrasi dan saling melengkapi informasi untuk menghasilkan suatu output yang baik.

2.1.3 Pengertian Teknologi Informasi

Menurut Turban, Rainer dan Potter (2009, p6), "*Information technology relates to any computer-based to that people use to work with information and to support the information and information processing needs of an organization*". Yang diartikan sebagai berikut: teknologi informasi berkaitan dengan segala sesuatu yang berbasis komputer yang digunakan orang untuk melakukan pekerjaan yang berhubungan dengan informasi untuk mendukung dan mengolah informasi tersebut sesuai dengan kebutuhan perusahaan.

Menurut O'Brien (2007, p6) teknologi informasi adalah teknologi pendukung dari sistem informasi, yaitu sistem berbasis TI yang mengelola komponen-komponennya berupa *hardware, software*, netware, dataware, dan brainware untuk melakukan transformasi data menjadi informasi.

Jadi teknologi informasi dapat disimpulkan sebagai *hardware, software,* netware, dataware, brainware, dan teknologi pemrosesan informasi lainnya untuk mendukung sistem informasi.

2.1.4 Infrastruktur Teknologi Informasi

Menurut Turban, Rainer, & Potter (2007, p6), "*Information technology infrastructure is the physical facilities, IT components, IT services, and IT personnel that support the entire organization.*"

Infrastruktur teknologi informasi pada sebuah organisasi terdiri dari sebuah perangkat fisik berupa *IT components, IT services, danIT management* yang mendukung keseluruhan organisasi. *IT components* terdiri dari computer *hardware*, *software*, dan teknologi komunikasi yang digunakan oleh personel teknologi informasi untuk menghasilja *IT services. IT services* meliputi manajemen data.

2.1.4.1 *Hardware*

Menurut O'Brien (2007, p6), *hardware* mencakup semua peralatan fisik yang digunakan dalam pemrosesan informasi. *Hardware* berkaitan dengan peralatan keras dengan media komunikasi yang menghubungkan beberapa jaringan dan memproses paket data sehingga transmisi data lebih efektif.

2.1.4.2 *Software*

Menurut O'Brien (2007, p104), *software* meliputi semua rangkaian perintah pemrosesan informasi. Konsep umum *software* ini tidak hanya rangkaian perintah informasi yang disebut program dengan hardware komputer pengendalian dan langsung, tapi juga rangkaian perintah pemrosesan informasi yang disebut prosedur yang dibutuhkan orang-orang.

2.1.4.3 Jaringan Komputer

Menurut Dede Sopandi (2008, p2), jaringan komputer adalah gabungan antara teknologi komputer dan teknologi telekomunikasi. Gabungan teknologi ini menghasilkan pengolahan data yang dapat didistribusikan, mencakup pemakaian database, *software* aplikasi dan peralatan *hardware* secara bersamaan. Secara geografis jaringan komputer dibedakan menjadi beberapa macam, sebagai berikut : *Local Area Network (LAN)*, *Metropolitan Area network (MAN)*, dan *Wide Area Network (WAN).*

2.1.4.4 Internet, Intranet, Ekstranet

Menurut McLeod dan Schell (2007, p.117), Internet adalah jaringan komputer yang tumbuh cepat dan terdiri dari jutaan jaringan, perusahaan, pendidikan, serta pemerintah yang menghubungkan ratusan juta komputer, serta pemakaian lebih dari dua ratus negara.

Menurut McLeod & Schell (2007, p.117), intranet adalah jaringan dalam organisasi yang menggunakan teknologi internet (seperti *server*, dan *browser web*, protokol jaringan, TCP/IP, database publikasi dokumen Hipermedia HTML, dan lain-lain) untuk menyediakan lingkungan yang mirip dengan internet didalam perusahaan untuk memungkinkan saling berbagai informasi, komunikasi, kerjasama, dan dukungan bagi proses bisnis.

Menurut McLeod & Schell (2007, p.117), ekstranet adalah hubungan jaringan yang menggunakan teknologi intranet untuk saling menghubungkan intranet pelanggannya, supplier dan mitra bisnis lainnya.

2.2 Risiko

2.2.1 Pengertian Risiko

Menurut Gondodiyoto (2007, p110) risiko adalah suatu *chances*, perusahaan dapat memperkecil risiko dengan melakukan antisipasi berupa kontrol, namun tidak mungkin dapat sepenuhnya menghindari adanya *exposure*, bahkan dengan struktur pengendalian maksimal sekalipun.

2.2.2 Jenis-Jenis Risiko

Menurut Gondodiyoto (2009, p110), risiko dapat dibedakan dalam beberapa jenis, yaitu :

a. Risiko Bisnis (*Business Risks*)

Risiko Bisnis adalah risiko yang dapat disebabkan oleh factor-faktor intern (permasalahan kepegawaian, berkaitan dengan mesin-mesin, dll) maupun *ekstern* (perubahan kondisi perekonomian, tingkat kurs yang berubah mendadak, dll) yang berakibat kemungkinan tidak tercapainya tujuan organisasi.

b. Risiko Bawaan (*Inherent Risks*)

Risiko Bawaan adalah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan, jika tidak ada pengendalian *intern*. Contohnya kegiatan kampus, jika tidak ada

absensi akan banyak mahasiswa yang tidak hadir.

c. Risiko Pengendalian (*Control Risks*)

Risiko pengendalian adalah masih adanya risko meskipun sudah ada pengendaluan. Contohnya meskipun sudah ada absensi tetapi tetap saja beberapa mahasiswa yang menitip absen.

d. Risiko Deteksi (*Detection Risks*)

Risiko deteksi adalah risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya *error* yang cukup atau materialitas atau adanya kemungkinan *fraud*.

e. Risiko Audit (Audit Risks)

Risiko audit adalah risiko risiko bahwa hasil pemeriksaan auditor ternyata belum mencerminkan keadaan sesungguhnya.

2.2.3 Penilaian Risiko

Menurut Jones, Federick, & Rama (2008, p170), penilaian risiko identifikasi dan analisis risiko yang mengganggu pencapaian sasaran pengendalian.

Menurut Gondodiyoto (2007, p116), penilaian risiko adalah salah satu langkah kritis dalam penyusunan *internal control* yang efektif, yaitu dalam memperkirakan ancaman yang mungkin dihadapi.

Kesimpulan dari definisi-definisi tersebut penilaian risiko adalah langkah efektif dalam memperkirakan ancaman yang mungkin akan dihadapi.

2.2.4 Karakteristik dan Wujud Risiko

Menurut Djojosoedarso (2005, p3), karakteristik risiko merupakan ketidakpastian atas terjadinya suatu peristiwa dan merupakan ketidakpastian bila terjadi akan menimbulkan kerugian.

Menurut Djojosoedarso (2005, p3), wujud dari risiko itu dapat bermacam- macam, antara lain :

a. Berupa kerugian atas harta milik/kekayaan atau penghasilan, misalnya diakibatkan oleh kebakaran, pencurian, pengangguran dan sebagainya.
b. Berupa penderitaan seseorang, misalnya sakit/cacat karena kecelakaan.
c. Berupa tanggung jawab hukum, misalnya risiko dari perbuatan atau peristiwa yang merugikan orang lain.
d. Berupa kerugian karena perubahan keadaan pasar,misalnya terjadi perubahan harga, perubahan selera konsumen dan sebagainya.

2.2.5 Upaya Penanggulangan Risiko

Menurut Djojosoedarso (2005, p4), upaya-upaya untuk menanggulangi risiko harus selalu dilakukan, sehingga kerugian dapat dihindari atau diminimumkan.

Sesuai dengan sifat dan objek yang terkena risiko, ada beberapa cara yang dapat dilakukan perusahaan untuk meminimumkan risiko kerugian, antara lain :

1. Melakukan pencegahan dan pengurangan terhadap kemungkinan terjadinya peristiwa yang menimbulkan kerugian.

2. Melakukan retensi, artinya mentolerir membiarkan terjadinya kerugian, dan untuk mencegah terganggunya operasi perusahaan akibat kerugian tersebut disediakan sejumlah dana untuk menanggulanginya.
3. Melakukan pengenadalian terhadap risiko.
4. Mengalihkan / memindahkan risiko kepada pihak lain.

2.3 Risiko Teknologi Informasi

2.3.1 Kategori Risiko Tesknologi Informasi

Menurut Hughes (2006, p36), dalam penggunaan teknologi informasi berisiko terhadap kehilangan informasi dan pemulihannya yang tercakup dalam 6 kategori, yaitu:

a. Keamanan

   Risiko yang informasinya diubah atau digunakan oleh orang yang tidak berwenang. Misalnya saja kejahatan komputer, kebocoran internal dan terorisme *cyber*.

b. Ketersediaan

   Risiko yang datanya tidak dapat diakses setelah kegagalan sistem, karena kesalahan manusia (*human error),* perubahan konfigurasi, dan kurangnya penggunaan arsitektur.

c. Daya Pulih

   Risiko dimana informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup, setelah terjadinya kegagalan dalam perangkat lunak atau keras,ancaman *eksternal*, atau bencana alam.

d. Performa

Risiko dimana informasi tidak tersedia saat diperlukan, yang diakibatkan oleh arsitektur terdistribusi, permintaan yang tinggi dan topografi informasi teknologi yang beragam.

e. Daya Skala

Risiko yang perkembangan bisnis, pengaturan *bottleneck,* dan bentuk arsitekturnya membuatnya tidak mungkin menangani banyak aplikasi baru dan biaya bisnis secara efektif.

f. Ketaatan

Risiko yang manajemen atau penggunaan informasinya melanggar keperluan dari pihak pengatur. Yang dipersalahkan dalam hal ini mencakup aturan pemerintah, panduan pengaturan perusahaan dan kebijakan internal.

2.3.2 Kelas-kelas Risiko Teknologi Informasi

Menurut Jordan & Silcock (2005, p49), risiko-risiko teknologi didefinisikan dalam 7 kelas, dimana pada setiap kasus, teknologi informasi dapat juga melakukan kesalahan, tetapi konsekuensi-konsekuensinya dapat berakibat negatif bagi bisnis. Kelas-kelas risiko yaitu :

1. Projects-failing to deliver

Risiko ini bersangkutan dengan gagalnya suatu proyek TI. Beberapa contoh dari gagalnya penyampaian proyek adalah menyelesaikan proyek yang ada telat / tidak pada waktunya, sumber daya dan biaya yang di konsumsi dalam penyelesaian proyek besar sehingga tidak efisien, mengganggu proses bisnis

selama proses implementasi, dan juga fungsi dari proyek tidak sesuai dengan keinginan dari yang diharapkan user.

2. *IT service continuity-when business operations go off the air*

   Risiko ini berhubungan dengan pelayanan TI yang ketinggalan zaman dan tidak dapat diandalkan sehingga mengganggu proses bisnis yang sedang berjalan. Biasanya berhubungan dengan sistem operasional dan produksi perusahaan serta kemampuan mereka untuk menyediakan kebutuhan dari user.

3. *Information assets-failing to protect and preserve*

   Risiko ini berhubungan khusus dengan kerusakan, kehilangan dan eksploitasi aset informasi yang ada dalam sistem. Dampaknya bisa sangat fatal bagi perusahaan, contohnya informasi yang penting bisa dicuri oleh perusahaan kompetitor, detail dari kartu kredit dapat dilihat oleh pihak yang tidak berwenang, sehingga dengan demikian akan merusak hubungan antara pelanggan dengan perusahaan. Ini tentunya akan sangat merugikan perusahaan.

4. *Service providers and vendors-breaks in the IT value chain*

   Risiko ini berhubungan dengan kemampuan dari *provider* dan *vendor.* Bila mereka gagal dalam menyediakan pelayanan yang baik bagi kita, maka akan berdampak significant bagi sistem TI perusahaan. Dampak lainnya berhubungan dengan dampak jangka panjang seperti kekurangan dalam penyediaan layanan TI bagi *user* perusahaan tersebut.

5. *Applications-flaky systems*

   Risiko ini berhubungan dengan kegagalan aplikasi TI yang diterapkan. Aplikasi biasanya berinteraksi dengan *user* dan dalam suatu perusahaan biasanya terdapat kombinasi antara *software* paket dan *software* buatan yang diintegrasikan menjadi satu.

6. *Infrastructure-shaky foundations*

   Risiko ini berhubungan dengan kegagalan dalam infrastruktur TI. Infrastuktur adalah suatu nama yang umum bagi komputer maupun jaringan yang sedang dipakai dan berjalan di perusahaan tersebut. Didalam infrastuktur juga termasuk *software,* seperti *Operation System* dan *Database Management System.*

   Kegagalan infrastuktur TI bisa bersifat permanen, ketika suatu komponen terbakar, dicuri, rusak maupun koneksi jaringannya sedang putus, maka dampak dari kegagalan tersebut tergantung dari ketahanan sistem yang ada. Apabila terdapat sistem yang sudah tidak kompatibel dengan model yang baru, maka sistem tersebut perlu diganti. Apabila risiko ini dapat ditangani secara rutin, maka itu merupakan suatu perencanaan jangka panjang yang baik.

7. *Strategic and energent-disabled by IT*

   Risiko ini berhubungan dengan kemampuan TI untuk memberitahukan strategi bisnis yang dilakukan. Dampak-dampak yang tidak langsung tetapi sangat significant dalam pelaksanaan bisnis secara luas. Risiko merupakan kemampuan dari perusahaan untuk terus bergerak maju kearah visi strategi, untuk tetap

kompetitif diperlukan kemajuan TI untuk dipahami dan dicocokan dengan potensi kesempatan eksploitasi bagi bisnis.

2.3.3 Langkah Pemecahan Risiko Teknologi Informasi

Menurut Jordan & Silcock (2005, p7), ada tiga langkah kunci dalam membuat risiko teknologi informasi dapat berjalan, yaitu dengan menempatkan diri anda dalam satu posisi dimana anda dapat hidup dengan risiko :

1) Anda perlu menempatkan kepemimpinan dan manajemen yang tepat pada tempatnya melalui teknologi informasi dan kerangka cara pengaturan risiko.
2) Anda perlu menggabungkan cara anda mengurus risiko informasi teknologi dengan mengadopsi sebuah pendekatan manajemen tas surat yang proaktif.
3) Anda perlu mengatur kompleksitas dengan secara aktif mengatur setiap jenis risiko informasi teknologi.

2.4 Manajemen Risiko

2.4.1 Pengertian Manajemen Risiko

Menurut Jones, Federick, & Rama (2008, p.193), manajemen risiko adalah kegiatan pemimpinan puncak mengidentifikasi, menangani, dan memonitori risiko bisnis yang dihadapi perusahaan mereka di masa yang akan datang.

2.4.2 Tugas Manajemen Risiko

Menurut Blokdjik (2008, p82), tugas manajemen risiko adalah mengelola risiko suatu proyek untuk risiko. Tujuannya adalah untuk

mengelola risiko bahwa dengan melakukan tindakan untuk menjaga hubungan ke tingkat yang dapat diterima dengan cara yang hemat biaya. Manajemen risiko meluputi: akses yang dapat dipercaya, tentang risiko yang tebaru, proses pengambilan keputusan didukung oleh kerangka analisis risiko dan proses evaluasi, memantau risiko, pengendalian yang tepat untuk menghadapi risiko.

2.4.3 Fungsi-Fungsi Pokok Manajemen Risiko

Menurut Djojosoedarso (2003, p14), fungsi pokok manajemen risiko terdiri dari:

1. Menemukan Kerugian Potensial

   Artinya berupaya untuk menemukan atau mengidentifikasi seluruh risiko murni yang dihadapi perusahaan, yang meliputi :

   a. Kerusakan fisik dari harta kekayaan perusahaan
   b. Kehilangan pendapatan atau kerugian lainnya akibat terganggunya operasi perusahaan.
   c. Kerugian akibat adanya tuntutan hukum dari pihak lain.
   d. Kerugian-kerugian yang timbul karena penipuan, tindakan-tindakan kriminal lainnya, tidak jujurnya karyawan.
   e. Kerugian-kerugian yang timbul akibat karyawan, meninggal dunia, sakit atau cacat.

2. Mengevaluasi Kerugian Potensial

   Artinya melakukan evaluasi dan penilaian terhadap semua kerugian potensial yang dihadapi perusahaan. Evaluasi dan penilaian ini akan meliputi perkiraan mengenai :

a. Besarnya kemungkinan frekuensi terjadinya kerugian, artinya memperkirakan jumlah kemungkinan terjadinya kerugian selama suatu periode tertentu atau berapa kali terjadinya kerugian tersebut selama suatu periode tertentu.

b. Besarnya bahaya dari tiap-tiap kerugian, artinya menilai kerugian yang diderita, yang biasanya dikaitkan dengan besarnya pengaruh kerugian tersebut, terutama terhadap kondisi finansial perusahaan.

3. Memiliki teknik atau cara yang tepat atau menentukan suatu kombinasi dari teknik - teknik yang tepat guna menanggulangi kerugian.

Pada pokoknya ada empat cara yang dapat dipakai untuk menanggulangi risiko, yaitu mengurangi kesempatan terjadinya kerugian, meretensi, mengasuransikan, dan menghindari. Tugas dari manajer risiko adalah memilih suatu cara yang paling tepat untuk menanggulangi suatu risiko atau memilih suatu kombinasi dara cara-cara yang paling tepat untuk menanggulangi risiko.

2.4.4 Implementasi Kemampuan Manajemen Risiko Teknologi Informasi

Menurut Artur Rot (2009, vol 2), *The objective of IT risk management is to protect Information Technology assets such as data, hardware, software, personnel and facilities from all external (e.g. natural disasters) and internal (e.g. technical failures, unauthorized access) threats so that the costs of losses resulting from the realization of such threats are minimized.* Yang diartikan sebagai

berikut: tujuan dari manajemen risiko TI adalah untuk melindungi aset Teknologi Informasi seperti data, hardware, software, personel dan fasilitas dari semua (kegagalan teknis misalnya, akses yang tidak sah) ancaman eksternal (bencana alam misalnya) dan internal sehingga biaya kerugian yang diakibatkan oleh realisasi ancaman tersebut diminimalkan.

Menurut Jordan & Silcock (2005, p60), kemampuan manajemen risiko teknologi informasi yang efektif adalah kemampuan manajemen yang memenuhi kebutuhan bisnis, dimana elemen desain penting yang harus dipertimbangkan adalah :

1. Strategi dan Kebijakan

   Strategi-strategi dan kebijakan-kebijakan manajemen risiko teknologi informasi diperlukan untuk dapat menentukan tujuan dari manajemen risiko teknologi informasi, memastikan cakupan area yang potensial dari risiko teknologi informasi dan menyediakan landasan peraturan dan prinsip-prinsip untuk mengelola risiko. Kebijakan manajemen risiko teknologi informasi harus didokumentasikan secara formal dan didukung oleh tim tata kelola teknologi informasi dan dikomunikasikan secara aktif kepada seluruh organisasi.

2. Peran dan Tanggung Jawab

   Peran yang perlu ditentukan terlebih dahulu dan sesudah itu orang yang tepat dan harus dipilih dan ditempatkan untuk melakukan peran tersebut.

   Beberapa hal yang perlu dipertimbangkan adalah :

a. Pemisahan tugas : untuk memastikan bahwa setiap peran kelas risiko independen menjalankan pemantauan dan melakukan tinjauan ulang.
b. Menyeimbangkan kebutuhan masukan untuk spesialis : kontribusi pengertian proses, sistem dan risiko spesifik, manajerial pembuat suatu keputusan mempertimbangkan semua faktor dan menentukan tindakan.
c. Mencocokan peran manajemen risiko teknologi informasi kedalam struktur dimana dia seharusnya ditempatkan. Misalnya, aktifitas perawatan manajemen risiko teknologi informasi harus sejalan dengan manajer proyek untuk risiko proyek.
d. Membuat peran manajemen risiko teknologi informasi yang baru ketika dibutuhkan. Misalnya, lintas fungsional bisnis dengan koordinasi peran secara berkelanjutan.
e. Mengalokasikan tanggung jawab bersama jika diperlukan dan memastikan semua tempat telah diambil.

3. Proses dan Pendekatan

Siklus hidup manajemen risiko memiliki beberapa langkah, yang dikembangkan dengan beberapa langkah yang berbeda untuk berbagai jenis risiko:

a. Identifikasi/Penemuan : Mendapatkan risiko teknologi informasi berdasarkan radar dari manajemen.
b. Penilaian/Analisis : Memahami risiko dalam konteks keseluruhan *portfolio* risiko teknologi informasi dan menilai

kemungkinan terjadinya dan dampak potensial terhadap bisnis.

c. Perawatan : Menentukan pilihan terbaik dari banyaknya program untuk menangani risiko, perencanaan dan menyelesaikan tindakan yang diperlukan.

d. Pemantauan dan Tinjauan : Menindaklanjuti untuk memastikan rencana apa yang telah dilakukan dan memahami adanya perubahan lebih lanjut dalam risiko dari *portfolio.*

4. Orang dan Performa

Manajemen risiko teknologi informasi juga tentang orang dan performa mereka. Kemampuan dan pengetahuan dari orang-orang dalam manajemen risiko teknologi informasi harus dikembangkan dan dipelihara.

Pengembangan dan pemeliharaan ini memerlukan beberapa kombinasi pendidikan dan pelatihan penanggulangan risiko teknologi informasi sesusai dengan peran dan tanggung jawab yang ada.

5. Implementasi dan Pengembangan

Orang tidak hanya akan menerima cara baru dalam pengelolaan risiko teknologi informasi tanpa pernah diberitahu mengapa diperlukan. Sebuah cerita yang meyakinkan pentingnya hal tersebut untuk organisasi dan apakah itu penting untuk organisasi.

2. 5 Metodologi Pengukuran Risiko Teknologi Informasi

Menurut Maulana & Supangkat (2006, p121), terdapat banyak metode yang bisa digunakan dalam penerapan manajemen risiko teknologi informasi, diantaranya menggunakan metode OCTAVE.

Metode OCTAVE memiliki varian yang lebih sederhana yang dikenal dengan nama OCTAVE-S.

Menurut Piya, Rens Scheepers, Wally Smith & Atif Ahmad (2011, vol 41), *OCTAVE, applied notably in the healthcare industry and the US military (West et al., 2002), is representative of ISRAs used by industry more generally.* Yang diartikan sebagai berikut: OCTAVE, diterapkan terutama dalam industri kesehatan dan militer AS (West et al., 2002), merupakan perwakilan dari ISRA yang lebih umum digunakan oleh industri.

2.5.1 OCTAVE-S

Alberts, C., Dorofee, A., Stevens, J., Woody. C. (2005, p5), OCTAVE-S adalah bentuk evaluasi risiko keamanan informasi yang bersifat *self – directin.* Metode ini memerlukan sebuah tim analisis untuk memeriksa risiko-risiko keamanan terhadap aset kritis organisasi dalam hubungannya dengan tujuan-tujuan bisnia, pada akhirnya melibatkan strategi perlindungan dan rencana mitigasi risiko berbasis aset, pada tingkat organisasional. Dengan mengimplementasikan hasil dari OCTAVE-S, sebuah organisasi dapat secara lebih baik melindungi semua aset terkait informasi dan meningkatkan posisi keamanan secara keseluruhan.

OCTAVE-S (The Operational Critical Threat, Asset, and Vulnerability Evaluation)-Small mampu mengelola risiko perusahaan dengan mengenali risiko-risiko yang mungkin terjadi pada perusahaan dan membuat rencana penanggulangan dan mitigasi terhadap masing-masing risiko yang telah diketahui.

Evaluasi risiko keamanan sistem informasi yang dilakukan oleh metode OCTAVE S bersifat komprehensif, sistematik, terarah dan dilakukan sendiri. Untuk mendukung dan memudahkan pelaksanaan analisis risiko dengan menggunakan metode OCTAVE-S, maka diperlukan suatu sistem berbasis komputer yang mampu melakukan analisis risiko terhadap keamanan perusahaan sesuai dengan langkah-langkah metode OCTAVE-S.

2.5.2 Fase, Proses, Aktivitas, dan Langkah Pada OCTAVE-S

Alberts, C., Dorofee, A., Stevens, J., Woody. C. (2005, vol 1) proses OCTAVE terdiri dari 3 tahap yaitu :

Tahap 1 : *Build Asset- Based Thread Profile*

Tahap 1 tim analisa mengidentifikasikan kriteria dampak evaluasi yang akan dipergunakan untuk mengevalusi risiko. Juga mengidentifikasi asset perusahaan yang penting dan mengevaluasi praktik keamanan yang sedang berjalan dalam perusahaan. Pada akhirnya, tim mengidentifikasi keamanan dan suatu profile ancaman untuk masing-masing aset yang kritis.

Tahap 2 : *Identify Infrastructure Vulnerabilities*

Tahap 2 ini tim analisa melaksanakan high level review dari infrastruktur perusahaan yang berfokus pada sejauh mana

infrastruktur mempertimbangkan keamanan. Tim analisa menganalisa bagaimana orang-orang menggunakan infrastruktur untuk megakses aset yang kritis, menghasilkan kelas kunci dari komponen seperti halnya siapa yang bertanggung jawab untuk mengatur dan memelihara komponen tersebut.

Tahap 3 : *Develop Security and Plans*

Tahap 3 tim analisa mengidentifikasi risiko ke aset kritis perusahaan dan memutuskan apa yang harus dilakukan terhadap aset kritis tersebut. Berdasarkan pada analisa dari informasi yang dikumpulkan, tim membuat strategi perlindungan untuk perusahaan dan rencana untuk mengurangi dan mengatasi risiko.

OCTAVE-S mempunyai 5 proses yang mana didalamnya terdiri dari 16 aktivitas dan 30 langkah, yaitu :

Tahap 1 : *Build Asset- Based Thread Profile*

Proses 1 : Mengidentifikasi Informasi Organisasi

1.1 Membangun Kriteria Evaluasi Dampak

Langkah 1 : mendefinisikan suatu pengukuran berdasarkan kualitasnya (tinggi, sedang, rendah) terhadap efek risiko yang akan dievaluasi dalam misi organisasi dan tujuan bisnis organisasi.

1.2 Mengidentifikasi Aset Organisasi

Langkah 2 : mengidenifikasi aset yang berhubungan dengan informasi dalam organisasi (informasi,sistem,aplikasi dan orang).

1.3 Mengevalusi Praktik Keamanan Organisasi

Langkah 3 :

a. Menentukan batasan pada setiap praktik keamanan dalam survey yang digunakan dalam organisasi.

b. Mengevaluasi praktik pengamanan dengan mempergunakan survey dari langkah sebelumnya.

Langkah 4 : Setelah menyelesaikan langkah 3 tentukan stoplight status (merah, kuning, hijau) untuk area praktik pengamanan.

Proses 2 : Membuat Profil Ancaman

2.1 Memilih Aset Kritis

Langkah 5 : Mengkaji ulang aset yang berhubungan dengan informasi yang telah diidentifikasi pada saat langkah dua dan memilih kurang lebih lima aset yang paling kritis dalam organisasi.

Langkah 6 : Memulai sebuah kertas kerja informasi aset kritis untuk setiap aset kritis. Catat nama aset kritis pada kertas kerja informasi aset kritis yang tepat.

Langkah 7 : Mencatat dasar pemikiran untuk memilih setiap aset kritis pada kertas kerja informasi aset kritis.

Langkah 8 : Mencatat deskripsi untuk setiap aset kritis pada kertas kerja informasi aset kritis. Pertimbangkan siapa saja yang menggunakan setiap aset kritis dan yang bertanggung jawab.

Langkah 9 : Mencatat aset yang terkait dengan setiap aset kritis pada kertas kerja informasi aset kritis. Pada kertas kerja identifikasi aset menentukan aset yang berhubungan dengan aset kritis.

2.2 Identifikasi Kebutuhan Keamanan Untuk Aset Kritis

Langkah 10 : Mencatat persyaratan pengamanan yang dibutuhkan untuk setiap aset kritis pada kertas kerja informasi aset kritis.

Langkah 11 : Untuk setiap aset kritis, mencatat persyaratan kemanan yang paling penting pada aset kertas kerja informasi aset kitis.

2.3 Identifikasi Ancaman Pada Aset Kritis

Langkah 12 : Lengkapi semua skema ancaman yang sesuai untuk setiap aset kritis. Tandai setiap bagian dari tiap skema untuk ancaman yang tidak dapatdiabaikan terhadap aset.

Langkah 13 : Mencatat contoh spesifik dari perilaku ancaman pada kertas kerja profil risiko untuk setiap kombinasi motif pelaku yang sesuai.

Langkah 14 : Mencatat kekuatan motif ancaman yang disengaja karena tindakan manusia. Catat seberapa besar kepercayaan terhadap perkiraan kekuatan atas motif pelaku.

Langkah 15 : Mencatat seberapa sering ancaman telah terjadi dimasa lal. Catat seberapa keakuratan data.

Langkah 16 : Mencatat area yang terkait untuk setiap sumber ancaman yang sesuai. Area yang terkait menjadi suatu skenario yang mengidentifikasikan seberapa spesifik ancaman dapat mempengaruhi aset kritis.

Tahap 2 : ***Identify Infrastructure Vulnerability***

Proses 3 : Memeriksa Perhitungan Infrastruktur yang Berhubungan dengan Aset Kritis

3.1 Memeriksa Jalur Aset

Langkah 17 : Memilih sistem yang menarik untuk setiap aset kritis, yaitu sistem yang paling berkaitan erat dengan aset kritis.

Langkah 18a : Memeriksa jalur yang digunakan untuk mengkases setiap aset kritis dan memilih kelas kunci dari komponen yang terkait untuk setiap aset kritis.

Langkah 18b : Menentukan kelas komponen yang berfungsi sebagai jalur aset (misalnya, komponen yang digunakan untuk mengirimkan informasi dan aplikasi dari sistem yang menarik untuk orang)

Langkah 18c : Menentukan kelas komponen, baik internal maupun eksternal ke jaringan organisasi, yang digunakan oleh orang (misalnya, pengguna, penyerang) untuk mengakses sistem.

Langkah 18d : Menentukan dimana informasi yang menarik dari sistem disimpan untuk membuat back up.

Langkah 18e : Menentukan sistem lain yang dapat mengakses informasi atau aplikasi dari *system of interest* dan kelas-kelas komponen mana yang dapat digunakan untuk mengakses informasi penting.

3.2 Menganalisa Proses yang Terkait Dengan Teknologi

Langkah 19a : Tentukan kelas komponen yang terkait dengan satu atau lebih aset kritis dan yang dapat memberikan akses ke aset tersebut.

Langkah 19b : Untuk setiap kelas komponen didokumentasikan dalam langkah 19a, perhatikan aset kritis mana yang terkait dengan kelas tersebut.

Langkah 20 : Untuk setiap kelas komponen didokumentasikan dalam langkah 19a, perhatikan orang atau kelompok yang bertanggung jawab untuk memelihara dan melindungi kelas komponen.

Langkah 21 : Untuk setiap kelas komponen didokumentasikan dalam langkah 19a, perhatikan sejauh mana kelas tersebut dapat bertahan terhadap serangan jaringan. Juga catat bagaimana kesimpulan tersebut diperoleh. Akhirnya dokumen konteks tambahan yang berhubungan dengan analisis infrastruktur.

Tahap 3: Develop Security Strategy And Plans

Proses 4 : Identifikasi dan Analisis Resiko

4.1 Mengevaluasi Dampak Ancaman

Langkah 22 : Menggunakan kriteria evaluasi dampak sebagai panduan, menetapkan nilai dampak (tinggi, sedang, atau rendah) untuk ancaman aktif setiap aset kritis.

4.2 Membangun Kriteria Kemungkinan

Langkah 23 : Tentukan ukuran kualitatif pengukuran (tinggi, sedang, atau rendah) terhadap kemungkinan terjadinya ancaman yang akan di evaluasi.

4.3 Mengevaluasi Peluang Ancaman

Langkah 24 : Menggunakan kriteria evaluasi probabilitas sebagai panduan, menetapkan nilai probabilitas (tinggi, sedang, atau rendah) untuk masing-masing ancaman aktif untuk setiap aset kritis.

Proses 5 : Mengembangkan Strategi Perlindungan dan Rencana Mitigasi

5.1 Menggambarkan Strategi Perlindungan Saat Ini

Langkah 25 : Mengirim status spotlight dari setiap area praktik keamanan yang sesuai dengan area yang terkait pada kertas kerja strategi perlindungan. Untuk setiap wilayah praktik keamanan, identifikasikan pendekatan organisasi saat ini untuk mengatasi area tersebut.

5.2 Memilih Pendekatan Mitigasi

Langkah 26 : Mengirim status spotlight dari setiap area praktik keamanan dari kertas kerja praktik keamanan ke “area praktik kemanan” bagian (langkah 26) dari setiap aset kritis dan kertas kerja profil risiko.

Langkah 27 : Pilih pendekatan mitigasi (mengurangi, menunda, menerima) untuk setiap risiko yang aktif. Untuk setiap risiko diputuskan untuk ditangani, lingkaran satu atau lebih area praktik keamanan untuk dilaksanakan kegiatan mitigasi.

5.3 Mengembangkan Rencana Mitigasi Risiko

Langkah 28 : Mengembangkan rencana mitigasi untuk setiap area praktik keamanan yang dipilih pada langkan 27.

5.4 Mengidentifikasi Perubahan Untuk Strategi Perlindungan

Langkah 29 : Tentukan apakah rencana mitigasi mempengaruhi strategi perlindungan. Catat setiap perubahan kertas kerja strategiperlindungan. Selanjutnya, meninjau ulang strategi perlindungan , termasuk perubahab yang diajukan.

5.5 Mengidentifikasi Langkah Selanjutnya

Langkah 30 : Tentukan apakah organisasi perlu melakukan penerapan hasil evaluasi ini dan mengembangkan sikap keamanan.

2.5.3 Hasil OCTAVE-S

Selama mengevaluasi OCTAVE,-S tim analisis melibatkan keamanan dari beberapa perspektif, memastikan bahwa rekomendasi yang dicapai sesuai dengan keseimbangan berdasarkan kebutuhan organisasi.

Hasil utama dari OCTAVE-S, yaitu:

1. Strategi perlindungan organisasi yang luas: Perlindungan strategi menguraikan secara singkat arah organisasi dengan mematuhi praktik keamanan informasi.
2. Rencana mitigasi risiko: rencana ini dimaksudkan untuk mengurangi risiko aset kritis untuk meningkatkan praktik keamanan yang di pilih.
3. Daftar tindakan: Termasuk tindakan jangka pendek yang dibutuhkan untuk menunjukkan kelemahan yang spesifik.

Hasil OCTAVE-S yang berguna lainnya, yaitu:

1. Daftar informasi penting terkait dengan aset yang mendukung tujuan bisnis dan sasaran organisasi.
2. Hasil survei menunjukkan sejauh mana organisasi mengikuti praktik keamanan yang baik.
3. Profil risiko untuk setiap aset kritis menggambarkan jarak antara risiko terhadap aset. Jadi, setiap tahap OCTAVE-S memproduksi hasil yang bermanfaat sehingga sebagian evaluasi akan menghasilkan informasi yang berguna untuk meningkatkan sikap keamanan organisasi.

2.5.4 Kelebihan OCTAVE–S

Kelebihan –kelebihan dari metode OCTAVE-S antara lain :

1. Sederhana dan terarah, karena memiliki ketetapan mengenai praktik dan lembar kerja untuk mendokumentasikan hasil permodelan.
2. Bersifat objektif, karena risiko didapat dari pihak yang terkait.
3. Mendokumentasikan dan mengukur risiko kemanan TI secara keseluruhan.
4. Pembentukan tim kerja lebih sederhana sehingga lebih tepat waktu.
5. Memiliki framework sehingga pengukuran sesuai dengan detail list yang telah ditentukan.

2.5.5 Kelemahan OCTAVE-S

1. Memakan waktu cukup lama, karena pengukuran risiko TI dilakukan secara keseluruhan.