BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Beberapa penelitian yang terkait dengan penelitian ini adalah[5] dengan studi kasus di Bapelkes Batam. Pada penelitian tersebut berfokus pada sistem informasi yang sudah diterapkan oleh instansi yang terkait, hasil penelitian instansi belum semua menerapkan manajemen risiko TI, didapatkan beberapa prosedur standar seperti kebijakan TI, sistem kolaborasi, audit sistem informasi, arsitektur, manajemen mitigasi tidak di kelola dengan baik. Selain itu, semua karyawan yang bekerja dalam bidang TI baik pengguna atau administrator TI belum terlatih dengan baik. [6] Pada penelitian ini melakukan pengukuran risiko untuk mengindentifikasi aset perusahaan, menganalisis risiko-risiko dan merencanakan strategi perlindungan keamanan. Hasil penelitian yaitu pengelolaan risiko teknologi informasi pada perusahaan agar dapat meminimalkan risiko. Maka diharapkan perusahaan dapat mengindentifikasi risiko yang mungkin terjadi dan mengatasi secara efisien dan efektif.[7] studi kasus pada kantor BAPPEDA Kabupaten Sleman, hasil penelitian upaya mitigasi yang dilakukan pada penelitian tersebut adalah merupakan saran yang telah mencakup ruang lingkup perencanaan, dan pengamanan sistem informasi.

Perbedaan penelitian ini dengan penelitian sebelumnya terletak pada objek yang diteliti yaitu Staf IT PMI cabang Yogyakarta. Oleh karena itu penelitian ini melakukan mengevaluasi risiko keamanan informasi manajemen pada Staff IT PMI cabang Yogyakarta untuk mengetahui ancaman risiko keamanan informasi terhadap aset-aset kritis dan membuat rencana mitigasi untuk mengurangi risiko yang mungkin terjadi.

2.2 Pengertian Risiko

Menurut [9] risiko keamanan informasi didefinisikan sebagai potensi output yang tidak diharapkan dari pelanggaran keamanan informasi, oleh ancaman keamanan informasi.

2.1.3 Jenis-Jenis Risiko

Menurut[10] terdapat dua jenis risiko seacara umum, yaitu :

a) Risiko Murni (*pure risk)*
Risiko murni adalah ketidakpastian terjadinya suatu kerugian atau dengan kata lain hanya ada suatu peluang merugi dan bukan suatu peluang keuntungan. Risiko murni adalah suatu risiko yang bilamana terjadi akan memberikan kerugian dan apabila tidak terjadi maka tidak menimbulkan kerugian namun juga tidak menimbulkan keuntungan. Contohnya pada risiko ini adalah kebakaran,kecelakaan.

b) Risiko Spekulasi (speculative risk)
Risiko spekulasi adalah risiko yang bisa kita mengharapkan terjadinya kerugian dan juga keuntungan. Yang biasanya ada pada dunia bisnis

2.3 Keamanan Informasi

Menurut [11] Keamanan data ialah penjagaan data dari segala ancaman yang barangkali berlangsung dalam upaya untuk menetapkan maupun menjamin kelangsungan bisnis, meminimalisasi resiko bisnis serta mengoptimalkan alias memacu pengembalian investasi serta kesempatan, contoh dari keamanan data bagi [11] ialah *physical security, personal security, operational security, communication security, network security*.

2.3.1 Tujuan Keamanan Informasi

Menurut [9] keamanan informasi memiliki tiga tujuan untuk mencapai tujuan utama yaitu :

1. Kerahasiaan. Perusahaan berusaha melakukan perlindungan data dan informasi dari orang-orang yang tidak berwenang.
2. Ketersediaan. Infrastruktur perusahaan adalah menyediakan data dan informasi bagi pihak-pihak yang memiliki wewenang.
3. Intergritas. Semua sistem informasi yang menjamin tidak adanya pengubahan data tanpa adan izi dari pihak yang berwenang.

2.4 Manajemen Risiko

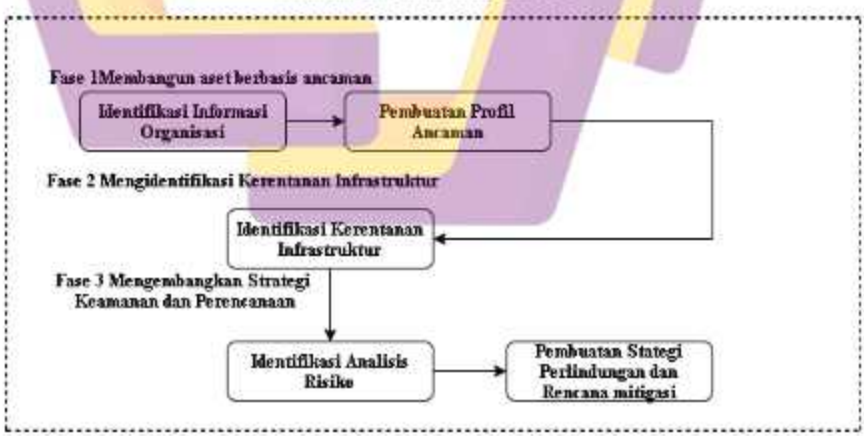
Menurut [9] manajemen risiko adalah menggambarkan pendekatan dimana pada

tingkat keamanan sumber daya informasi perusahaan dibandingkan dengan risiko yang dihadapinya. Manajemen keamanan informasi memiliki empat tahap yaitu mengidentifikasi risiko yang disebabkan oleh ancaman, menentukan kebijakan keamanan informasi dan mengimplementasikan pengendalian untuk mengatasi risiko-risiko tersebut.

2.5 Metode Ocatave-S

Octave-S adalah varian dari metode OCTAVE, yang dikembangkan untuk kebutuhan organisasi kecil. Untuk mengelola risiko keamanan sistem informasi, perlu dilakukan penilaian risiko untuk mengurangi kerugian yang akan terjadi. Salah satu cara untuk menilai risiko keamanan suatu organisasi atau sistem informasi perusahaan adalah OCTAVE-S (Operational Critical Threats, Assets and Vulnerability Assessment)-Small skala kecil untuk mengelola risiko perusahaan dengan memahami risiko yang mungkin terjadi di perusahaan dan mitigasi. Risiko oleh[4]. Penilaian risiko keamanan informasi yang dilakukan dengan metode OCTAVE-S bersifat komprehensif, sistematis, tepat sasaran dan dilakukan secara independen. Mendukung dan mempromosikan penggunaan metode OCTAVE-S untuk analisis risiko. Dengan mengimplementasikan hasil-hasil dari OCTAVE-S, sebuah instansi berusaha melindungi semua informasi dengan lebih baik dan meningkatkan keseluruhan bidang keamanan. Dalam metode OCTAVE-S memiliki 3 fase. Seperti gambar dibawah ini :

Gambar 2. 1 fase-fase octave-s



1. Fase 1 : Membangun profil ancaman berdasarkan aset

Terdapat dua proses yaitu mengidentifikasi informasi organisasi dan proses pembuatan profil ancaman.

2. Fase 2 : Mengidentifikasi kerentanan Infrastruktur

Data proses ini hanya memiliki satu proses yaitu melakukan perhitungan aset kritis yang masih berhubungan dengan aset instansi.

3. Fase 3 : Mengembangkan strategi keamanan dan perencanaan

Pada fase ini terdapat dua yaitu membangun kemungkinan kriteria evaluasi dan mengindentidikasi dan menganalis risiko.

Fase-fase evaluasi OCTAVE-S dapat dilihat gambar dibawah ini

2.5.1 Hasil OCTAVE-S

Menurut[4] mengevaluasi OCTAVE-S untuk memastikan bahwa rekomendasi yang dicapai sesuai dengan keseimbangan berdasarkan kebutuhan organisasi. Hasil dari OCTAVE-S ada tiga:

a. Daftar informasi penting terkait aset yang mendukung tujuan bisnis organisasi
b. Hasil survei menunjukan sejauh mana dalam mengikuti praktek keamanan yang baik.
c. Profil risiko untuk setiap kritis menggambarkan jarak antara risiko terhadap aset.

Dalam tahapan OCTAVE-S membuat hasil yang bermanfaat sehingga sebagian evaluasi akan menghasilkan informasi yang berguna untuk keamanan organisasi.