BAB 1

PENDAHULUAN

1.1. Latar Belakang

Dunia yang berkembang pada saat ini sangat membantu banyak kalangan pekerjaan khususnya dibidang teknologi informasi. Banyak perusahaan berlomba – lomba untuk memberikan yang terbaik dan kepercayaan kepada *client* yang dimiliki agar dapat merasa nyaman dan tenang untuk memberikan kepercayaan kepada perusahaan tersebut untuk mengelola sistem informasi yang ada khususnya dalam bidang sistem informasi manajemen risiko. Untuk itu, maka akan diadakan audit sistem informasi manajemen risiko untuk melihat seberapa penting pengaturan risiko yang ada dalam sebuah perusahaan.

Menurut *Appley dan Oey Liang Lee* (2010:16) manajemen adalah tekni yang dimiliki oleh orang untuk memberikan pengarahan, mempengaruhi, mengawasi dan mengorganisasikan komponen – komponen yang ada dan saling menunjukan untuk dapat mencapai tujuan yang dimaksud yang telah ditentukan sebelumnya.

Menurut Djohanputro (2008;43) risiko adalah proses dalam mengidentifikasi, mengukur, memantau dan melakukan pengembangan cara lain dalam penanganan risiko, memonitoring dan melakukan pengendalian dalam penanganan risiko.

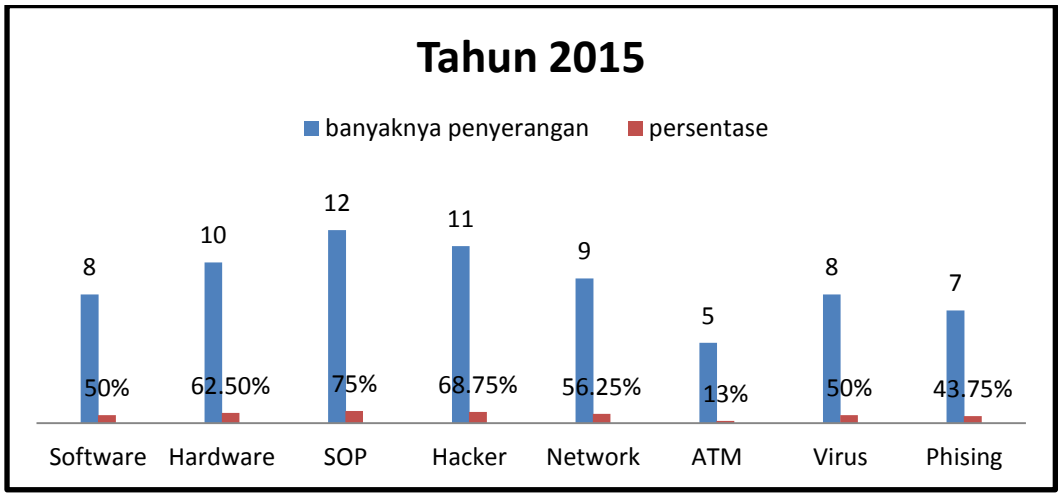
Dalam penanganan manajemen risiko ini, risiko itu sendiri dibagi menjadi beberapa bagian seperti risoko yang bersifat *low*, *medium* dan *high*. Maka untuk

kedepannya, perusahaan dapat melihat risiko mana yang akan dilakukan penangan terlebih dahulu agar risiko itu dapat diminimalisasikan agar perusahaan dapat terus berkembang sesuai dengan penanganan risiko dari pihak internal perusahaan tersebut.

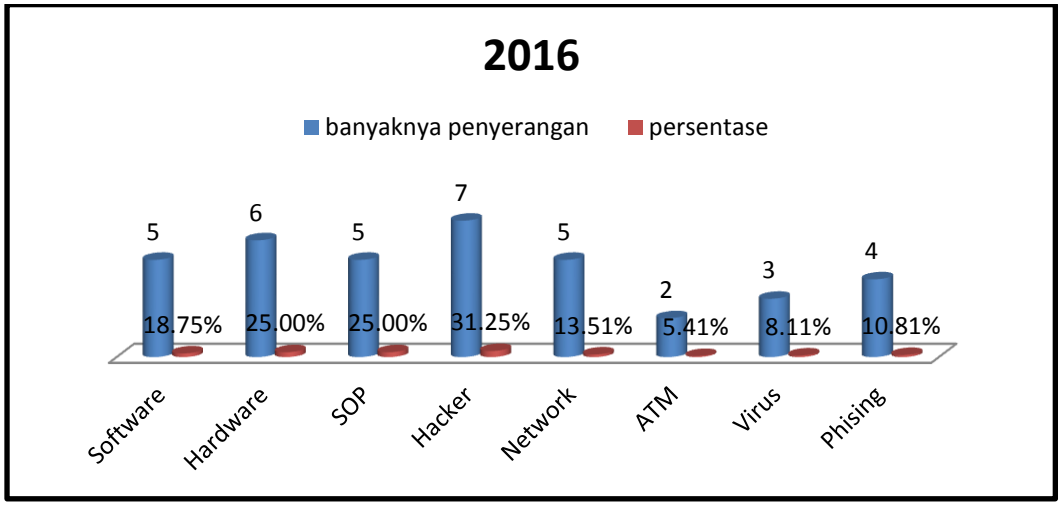
Risiko itu sendiri adalah kejadian yang dapat diminimalisasikan tetapi tidak dapat dihindari oleh semua orang. Maka dari itu, risiko dapat dideteksi sesuai dengan kejadian yang pernah terjadi atau yang belum pernah terjadi.

Ini adalah beberapa kejadian yang pernah terjadi pada bank xyz dalam penyerangan pihak yang tidak berkepentingan , virus , software dan sebagainya. Dapat dilihat dari grafik yang pernah terjadi pada tahun 2016 dan 2017 sampai pada bulan juli 2017:

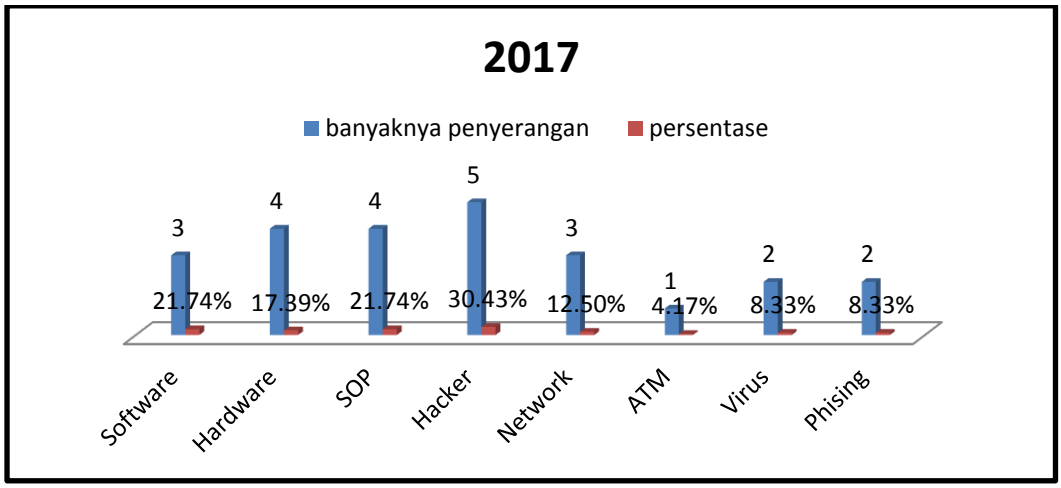
Berikut adalah beberapa kejadian yang terjadi pada bank xyz dalam penyerangan pihak yang tidak berkepentingan untuk mencoba mengambil data dan informasi yang dimiliki oleh bank tesebut. Dapat dilihat data – data dari tahun 2015 sampai 2017 untuk macam – macam penyerangan ada sudah di-*record* oleh bank terkait:



Gambar 1.1 Penyerangan pada pada tahun 2015 pada bank xyz



Gambar 1.2 Penyerangan pada tahun 2016 pada bank xyz



Gambar 1.3 Penyerangan pada tahun 2017 pada bank xyz

Dari gambar diatas, dapat dilihat bahwa cukup besar penyerangan yang dicoba oleh pihak yang tidak berkepentingan untuk mengambil data dan informasi yang ada pada bank terkait. Dari tahun 2015 – 2017 dapat dilihat bahwa sudah banyaknya perbaikan – perbaikan yang dilakukan oleh pihak bank untuk menjadi lebih baik dalam pengelolahan keamanan sistem informasi yang ada pada bank tersebut. Untuk itu, maka penulis akan melakukan penelitian lebih lanjut mengenai keamanan sistem informasi dan juga peran TIK dalam menjalankan keamanan sistem informasi pada bank xyz.

Dari gambar diatas , maka tujuan dari penelitian ini adalah menggunakan framework ISO 27001 yang terkait pada keamanan sistem informasi yang terkait pada bank xyz. Tujuan dari menggunakan ISO 27001 adalah untuk mempermudah dalam menganalisis sistem informasi yang ada pada bank xyz. Keuntungan dalam penerapan ISO 27001 adalah sebagai berikut :

1. Membantu organisasi terkait dengan kesesuaian terhadap kebutuhan standar keamanan informasi yang sudah teruji (best practice dalam pengamanan informasi)
2. Membuat pengaruh positif dalam hal citra perusahaan, nilai, dan persepsi yang baik dari pihak lain
3. Memastikan bahwa organisasi memiliki kontrol terkait keamanan informasi terhadap lingkungan proses bisnisnya yang mungkin menimbulkan risiko atau gangguan.
4. Meningkatkan kepercayaan pelanggan, pihak ketiga, dan seluruh stakeholder yang ada terhadap pelayanan yang diberikan melalui organisasi.
5. Membantu organisasi dalam menjalankan perbaikan yang berkesinambungan di dalam pengelolaan keamanan informasi.
6. Membuat pelaksanaan setiap proses menjadi lebih sistematis dan merubah budaya kerja organisasi.
7. Meminimalkan resiko melalui proses risk assessment yang professional, terstandarisasi dan komprehensif dalam kerangka manajemen resiko
8. Meningkatkan efektivitas dan keandalan pengamanan informasi

9. Diferensiasi pasar
10. Salah satu standar pengamanan informasi yang diakui di seluruh dunia
11. Kemungkinan rendahnya pembayaran premi asuransi yang harus dibayar kepada perusahaan asuransi karena standar yang sudah teruji.
12. Patuh terhadap hukum dan undang-undang seperti UU ITE, dll
13. Meningkatkan profit perusahaan
14. Menunjukkan tata kelola yang baik dalam penanganan informasi
15. Manajemen senior memiliki tanggung jawab keamanan informasi, sehingga staf lebih fokus terhadap tanggungjawabnya.
16. Adanya review yang independen terkait ISMS dengan adanya audit setiap tahun

menurut *ISO* 27001 , ada empat tahapan dalam melakuakan implementasi *ISO* 27001. Tahapan - tahapan ini dibagi menjadi beberapa bagian seperti :

1. *Plan:* pada tahap perencanaan ini , dalam fase ini akan dilihat permasalahan - permasalahan yang ada dalam sebuah perusahaan / organisasi.
2. *Do* (Penerapan dan pengoprasian SKMI) : Menerapkan dan mengoprasikan kebijakan , pengendalian , proses dan prosedur SKMI.
3. *Check* (Pemantauan dan pengkajian SKMI) : Mengases dan , apabila berlaku , mengukur kinerja proses terhadap kebijakan , sasaran SKMI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian

4. *Act* (Peningkatan dan pemeliharaan SKMI) : Mengambil tindakan korektif dan pencegahan bedasarkan hasil internal audit SKMI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SKMI.

Sumber: 16137_SNI *ISO_IEC* 27001_2009.PDF

1.2. Perumusan Masalah

Maka adapun rumusan masalah dalam Analisis Sistem Informasi untuk Bank XYZ antara lain sebagai berikut:

1. Bagaimana cara pengaturan dan pemeliharaan serta menjaga aset yang sudah ada?

   Menurut Evan Wheeler 2011 dalam dalam buku *security risk management* mengatakan bahwa dalam lingkup teknologi, ada beberapa area risiko utama (beberapa contoh tercantum) yang dapat digunakan untuk mengkategorikan jenis risiko yang serupa. Pengelompokan risiko ini membantu untuk mengidentifikasi risiko serupa dalam latihan pemodelan dan untuk tujuan pelaporan.

   1. Manajemen aset
   2. Keberlangsungan bisnis
   3. Manajemen perubahan
   4. Vendor dan *outsourcing*
   5. Perlindungan privasi dan data
   6. Fisik dan lingkungan

   Misalnya, risiko keamanan di area pengelolaan perubahan mungkin termasuk perubahan yang tidak sah terhadap lingkungan atau mungkin

juga karena mengabaikan jendela perawatan yang ditunjuk. Risiko keamanan informasi biasanya muncul di banyak domain dan berbagai area risiko di bawah domain tersebut, jadi penting untuk menambahkan area risiko yang sesuai untuk organisasi Anda. Masalah operasional, kepatuhan, dan hukum biasanya berada di urutan teratas daftar profesional keamanan, namun kami juga harus mempertimbangkan faktor lain, seperti ancaman fisik terhadap fungsi alih daya atau ketidakmampuan untuk memulihkan data selama situasi bencana. Semua ini mungkin berada di bawah payung keamanan informasi untuk diidentifikasi dan diawasi, namun pertanggungjawabannya terletak pada pemilik domain risiko lainnya untuk memfasilitasi kualifikasi risiko dan mengawasi kemajuan rencana mitigasi untuk ditangani di tingkat perusahaan.

2. Bagaimana cara memelihara dan membatasi akses kontrol dalam penanganan keamanan sistem informasi pada bank XYZ?

   Dalam ancaman terhadap keamanan sistem informasi , harus adanya akese kontrol yang digunakan untuk pengamanan sistem informasi. Menurut Evan wheeler 2011 pada bukunya *security risk management* mengatakan bahwa Ketika kita berbicara tentang mengamankan data, kita perlu memikirkan kontrol dalam tiga keadaan informasi:

   1. Dalam Transit: Ini mengacu pada data yang dikirimkan secara elektronik antara sistem atau transportasi fisik. Biasanya, ini termasuk keamanan jaringan dan kontrol keamanan fisik Anda.

2. Dalam Proses: Ini mengacu pada perlindungan data karena sedang digunakan oleh sistem atau aplikasi. Misalnya, ketika pengguna memasukkan data ke dalam bentuk, bagaimana data tersebut disaring dan diuraikan, bagaimana cara menyimpannya dalam memori saat diproses, dan bagaimana cara membuatnya tersedia bagi pengguna lain?
3. *At Rest*: Proteksi ini biasanya berfokus untuk melindungi data tempat penyimpanannya, entah itu database atau tape backup. Kontrol tipikal untuk keadaan ini meliputi Access Controls, Encryption, dan Physical Protections. Untuk setiap keadaan yang dapat diambil data, ada daftar panjang ancaman terhadap informasi tersebut.

Kategori utama adalah:

a. Pengungkapan yang tidak sah, seperti pelanggaran data
b. Korupsi, seperti modifikasi rekam data yang tidak disengaja
c. Denial of Service, seperti serangan yang membuat sumber daya tidak tersedia.
d. Ketidakmampuan untuk Membuktikan Sumber Serangan,seperti penggunaan akun bersama untuk melakukan aktivitas yang tidak sah. Perhatikan bahwa tiga kategori pertama dipetakan dalam Kerahasiaan, Integritas, dan Ketersediaan, dan keempat kategori memetakan ke akuntabilitas.

3. Bagaimana pengaturan komunikasi operasional yang ada di dalam bank XYZ?

   Dalam buku Michael E. Whitman dan Herbert J. Mattord yang berjudul Principle of information security 4th pada halaman 162 dikatakan bahwa organisasi harus berkomunikasi dengan pengguna sistem selama pengembangan program keamanan, membiarkan mereka mengetahui bahwa perubahan akan terjadi. Ini termasuk mengkomunikasikan jadwal dan jadwal pelaksanaan, serta tanggal, waktu, dan lokasi briefing dan pelatihan yang akan datang. Mereka yang membuat perubahan harus menguraikan tujuan dari perubahan yang diajukan dan menjelaskan bagaimana perubahan ini akan memungkinkan setiap orang untuk bekerja dengan lebih aman. Dalam hal ini , permasalahan yang terjadi pada bank xyz sering adanya perubahan yang datang secara tiba-tiba dan juga kurang adanya komunikasi.

1.3. Tujuan Penelitian

Dari rumusan masalah diatas, maka tujuan dari penelitian adalah sebagai berikut:

1. Pengaturan dan penjagaan aset sesuai dengan SOP yang berlaku.

   Dalam buku principles of information security 4th hal 43 mengatakan bahwa sumber daya organisasi yang terlindungi. Aset bisa jadi logis, seperti situs Web, informasi, atau data; atau aset bisa bersifat fisik, seperti seseorang, sistem komputer, atau benda berwujud lainnya. Aset, dan terutama aset informasi, merupakan fokus upaya keamanan. Oleh karena itu, tujuan dari penelitian ini adalah untuk melihat sejauh mana aset yang

dapat dijaga dan informasi yang dapat dijaga sesuai dengan ketentuan dari penerapan yang telah dilakukan oleh bak xyz.

2. Untuk memonitoring akses kontrol yang ada sudah sesuai dengan SOP dalam bank XYZ.

   Dalam buku principles of information security 4th hal 43 mengatakan bahwa kemampuan subjek atau objek untuk menggunakan, memanipulasi, memodifikasi, atau mempengaruhi subjek atau objek lain. Pengguna resmi memiliki akses legal ke sistem, sedangkan hacker memiliki akses ilegal ke sistem. Kontrol akses mengatur kemampuan ini. Hal – hal inilah yang harus dijaga pada bank terkait agar tidak adanya hak akses yang bersifat illegal yang mencoba mencoba membobol server dan pegambilan data yang bersifat kerahasian dari bank terkait.

3. Untuk Melihat sejauh mana komunikasi dan operasional yang sudah dijalankan pada bank xyz.

   Menurut Evan Wheeler 2011 hal 153 , apabila komunikasi dan operasional tidak dijakankan sesuai dengan ketentuan yang sudah ada pada perusahaan , maka apabila terjadi hal yang diluar pemikiran perusahaan, maka perusahaan mungkin mempertimbangkan sebuah proses atau kontrol prosedural dari pada kontrol teknis, namun Anda kemudian harus mempertimbangkan bagaimana keputusan tersebut dapat mempengaruhi efektivitas operasional.

   1) Pertimbangkan biaya
   2) Tidak menerapkan kontrol
   3) Pengurangan efektivitas operasional

4) Implementasi

5) Sumber daya tambahan

6) Pendidikan dan Pelatihan

Kapan pun Anda merekomendasikan kontrol keamanan teknis untuk mengurangi risiko, Anda harus memperhitungkan biaya langsung dan tidak langsung. Ada biaya awal perangkat keras, perangkat lunak, layanan profesional, dan sebagainya, serta biaya selama pemeliharaan dan dukungan.

1.4. Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Untuk mengetahui keamanan aset yang ada pada bank xyz.
2. Untuk melihat akses kontrol yang sudah ada apakah sudah sesuai dengan SOP yang berlaku pada bank xyz.
3. Untuk memastikan komunikasi berjalan dengan lancar agar operasional dapat berjalan selaras dengan bisnis yang ada pada bank xyz.

1.5. Ruang Lingkup

Ruang lingkup penelitian ini adalah sebagai berikut:

- Memberikan Kuisioner kepada pengguna sistem informasi yang ada di Bank XYZ.
- Melakukan sesi wawancara kepada pihak terkait yang berada di Bank XYZ.
- *Module-module* sistem informasi, *journal*, buku dan data yang sudah valid untuk dijadikan refrensi dalam penulisan thesis untuk kedepannya.