**Nama : Muhammad Rio Pratama (1810512002)**

**Khusnul Khotimah (1810512031)**

**Ahmad Ghani Fadillah (1810512072)**

**Allvira Arianti Amir H. (1810512078)**

**Kelas : Manajemen Risiko Teknologi Informasi**

**Hari, Tanggal : Selasa, 23 Maret 2021**

**TUGAS 1**

1. Mengulas mengenai hukum-hukum yang menyangkut tentang TI dan regulasinya. (Bisa data konsumen, kebijakan *privacy* dan undang-undang yang melindungi konsumen dalam bertransaksi).
2. Jelaskan prinsip-prinsip keamanan sistem.
3. Apa saja ancaman-ancaman keamanan sistem.
4. Apa yang dimaksud dengan Indeks KAMI (Indeks Keamanan Informasi).
5. Apa yang kegunaan/ manfaat dari Indeks KAMI (Indeks Keamanan Informasi).
6. Jelaskan mengenai pengukuran dengan menggunakan Indeks KAMI (Indeks Keamanan Informasi).
7. Apa kaitan antara keamanan sistem dengan manajemen risiko.

**JAWAB**

1. Dikarenakan semakin berkembangnya teknologi informasi yang semakin pesat, maka, peraturan hukum dalam pemanfaatan teknologi informasi pun akan sangat dibutuhkan. Berikut beberapa undang-undang yang melindungi konsumen dalam melakukan transaksi:
2. Pasal 8 Ayat 1 Huruf (F) Undang Undang No. 8 Tahun 1999 tentang perlindungan konsumen terkait informasi yang tidak benar dalam memperdagangkan barang atau jasa yang tidak sesuai dengan label, etiket, keterangan, iklan atau promosi penjualan barang atau jasa tersebut. Ketidaksesuaian spesifikasi barang yang konsumen terima dengan yang ada dalam foto atau iklan penawaran barang merupakan bentuk pelanggaran/larangan bagi pelaku usaha. Menurut pasal 4 huruf (h) UU 8/1999, konsumen berhak mendapatkan kompensasi, ganti rugi dan/atau penggantian apabila barang atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak sebagaimana mestinya.
3. Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengatur beberapa ketentuan yang merupakan bentuk perlindungan hukum kepada konsumen pengguna transaksi ECommerce. Bentuk perlindungan hukum tersebut adalah sebagai berikut :
4. Pasal 2 UU ITE, undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah indonesia maupun di luar wilayah hukum indonesia yang memiliki akibat hukum di Indonesia yang merugikan kepentingan Indonesia.
5. Pasal 9 UU ITE, pelaku usaha yang menawarkan produk melalui sistem elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen dan produk yang ditawarkan. Yang dimaksud dengan informasi lengkap dan benar adalah:
6. Informasi yang memuat identitas serta status subjek hukum dan kompetensinya baik sebagai produsen, pemasok, penyelenggara ataupun perantara.
7. Informasi lain yang menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian serta menjelaskan barang dan atau jasa dalam yang ditawarkan seperti nama, alamat dan deskripsi barang/jasa.
8. Perlindungan Hukum ditinjau dari UU PK. Konsumen dalam berbagai segi merupakan pihak yang lemah kedudukannya bila dibandingkan pelaku usaha, konsumen seringkali tidak memiliki posisi tawar jika berhadapan dengan pelaku usaha. Oleh karena itu, diperlukan suatu aturan yang dapat melindungi kepentingan konsumen agar tidak dirugikan atu diperlakukan sewenangwenang oleh pelaku usaha. UU PK menjami adanya epastian hokum untuk memberikan perlindungan kepada konsumen seperti tercantum dalam Pasal 1 Angka (1) UU PK. UU PK memberikan perlindungan kepada setiap konsumen yang merasa hak-haknya dilanggar atau dirugikan oleh pelaku usaha. Dalam UU PK ditentukan secara rinci hak-hak konsumen yang berlaku pula bagi konsumen pengguna transaksi elektronik/E-*Commerce*.
9. Sistem adalah sebuah aset dari organisasi yang penting. Tanpa sebuah sistem maka organisasi akan mengalami keruntuhan sedikit demi sedikit karena tidak ada batasan yang menjadi acuan dalam menerapkan sebuah proses bisnis. Maka dari itu, berikut adalah prinsip-prinsip keamanan sistem berdasarkan CIA *Triad* yang dapat diterapkan pada sebuah organisasi:
10. *Confidentiality*: pada bagian ini menetapkan sebuah kerahasiaan dalam menyimpan aset informasi organisasi. Informasi dapat tersedia dan diakses oleh orang-orang yang memiliki akses dan membutuhkannya. Hal ini dapat dilakukan dengan cara mengenkripsi informasi yang akan disebarkan atau menolak akses bagi orang-orang yang tidak pantas untuk mendapatkannya. Prinsip ini perlu diterapkan untuk mencegah akses ke semua lokasi perangkat.
11. *Integrity*: pada bagian ini menyediakan jaminan bahwa data tersebut akurat dan dapat dipercaya. Informasi hanya dapat ditambahkan atau diolah oleh orang-orang yang memiliki akses. Prinsip ini perlu diterapkan untuk mengizinkan atau menolak sebuah akses ke data yang akan diteruskan ke perangkat lain.
12. *Availibility*: pada bagian ini memiliki kemampuan untuk mengakses sebuah aset informasi yang ada atau tidak. Namun dengan catatan, jika informasi tidak dapat diakses, maka informasi tersebut menjadi tidak berguna. Akses data yang tidak tersedia akan mengakibatkan buruknya sebuah data yang rusak.

3. Pada era berkembangnya sistem informasi dan teknologi yang cepat, keamanan sebuah informasi sangat penting dan harus diperhatikan. Jika sebuah informasi itu bisa di akses oleh orang yang tidak bertanggung jawab maka bisa mengakibatkan ketidakakuratan informasi dan juga penyalahgunaan informasi. Maka dari itu keamanan informasi sangat penting untuk mencegah ancaman-ancaman apa saja yang mungkin bisa terjadi. Berikut ancaman-ancaman keamanan sistem:

1. Ancaman aktif
2. Pencurian data: jika informasi penting yang terdapat dalam database dapat diakses oleh orang yang tidak berwenang maka hasilnya dapat kehilangan informasi atau uang.
3. Penggunaan sistem secara illegal: orang yang tidak berhak mengakses informasi pada suatu sistem yang bukan menjadi hak-nya, dapat mengakses sistem tersebut. Penjahat komputer jenis ini umumny a adalah hacker yaitu orang yang suka menembus sistem keamanan dengan tujuan mendapatkan data atau informasi penting yang diperlukan, memperoleh akses ke sistem telepon, dan membuat sambungan telepon jarak jauh secara tidak sah.
4. Penghancuran data secara illegal: orang yang dapat merusak atau menghancurkan data atau informasi dan membuat berhentinya suatu sistem operasi komputer. Penjahat komputer ini tidak perlu berada ditempat kejadian.
5. Modifikasi secara illegal: perubahan-perubahan pada data atau informasi dan perangkat lunak secara tidak disadari. Jenis modifikasi yang membuat pemilik sistem menjadi bingung karena adanya perubahan pada data dan perangkat lunak disebabkan oleh progam aplikasi yang merusak.
6. Ancaman pasif
7. Kegagalan sistem: kegagalan sistem atau kegagalan software dan hardware dapat menyebabkan data tidak konsisten, transaksi tidak berjalan dengan lancar sehingga data menjadi tidak lengkap atau bahkan data menjadi rusak. Selain itu, tegangan listrik yang tidak stabil dapat membuat peralatan-peralatan menjadi rusak dan terbakar.
8. Kesalahan manusia: kesalahan pengoperasian sistem yang dilakukan oleh manusia dapat mengancam integritas sistem dan data.
9. Bencana alam: bencana alam seperti gempa bumi, banjir, kebakaran,hujan badai merupakan faktor yang tidak terduga yang dapat mengancam sistem informasi sehingga mengakibatkan sumber daya pendukung sistem informasi menjadi luluhlantah dalam waktu yang singkat.

4. Indeks KAMI (Keamanan Informasi) merupakan aplikasi yang digunakan sebagai alat bantu untuk menganalisa dan mengevaluasi tingkat kesiapan (kelengkapan dan kematangan). Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada Pimpinan Instansi. Implementasi Indeks KAMI dilakukan oleh penyelenggara layanan publik secara elektronik melalui bimbingan teknis, asesmen, dan konsultasi. Adapun penerapan keamanan informasi di sebuah organisasi harus sesuai dengan kriteria pada SNI ISO/IEC 27007, yaitu:

1. Tata Kelola
2. Pengelolaan Risiko
3. Kerangka Kerja
4. Pengelolaan Aset
5. Aspek Teknologi

5. Adapun manfaat / kegunaan dari indeks KAMI (Keamanan Informasi) adalah:

1. Mencegah ancaman-ancaman dari dalam maupun luar yang mengakibatkan terjadinya kerusakan dalam sistem.
2. Melindungi data dan juga informasi perusahaan atau organisasi dari orang-orang yang tidak bertanggung jawab.
3. Meyakinkan bahwa data dan informasi perusahaan hanya dapat digunakan oleh orang yang berhak menggunakannya.
4. Menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.

6. Pengukuran dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2009, yang disusun kembali menjadi 5 (lima) area di bawah ini:

1. Tata Kelola Keamanan Informasi, Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
2. Pengelolaan Risiko Keamanan Informasi, Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
3. Kerangka Kerja Keamanan Informasi, Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
4. Pengelolaan Aset Informasi, Bagian ini mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut; dan
5. Teknologi dan Keamanan Informasi, Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Proses evaluasi akan membahas sejumlah aspek yang dibutuhkan untuk mencapai tujuan utama dari pengamanan di area tersebut. Setiap aspek tersebut memiliki karakteristik tersendiri terkait dengan pentahapan penerapan pengamanan sesuai dengan standar SNI ISO/IEC 27001:2009. Aspek yang dibahas (disampaikan dalam konteks pertanyaan) terdiri dari bentuk kerangka kerja dasar keamanan informasi, efektivitas dan konsistensi penerapannya, sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi.Bentuk pengamanan terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar SNI ISO/IEC 27001:2009.

7. Keamanan sistem adalah sebuah langkah yang ditempuh untuk mengamankan dan menjaga sebuah sistem komputer dari gangguan dan segala ancaman yang membahayakan yang melingkupi keamanan data atau informasinya. Sedangkan manajemen risiko adalah suatu langkah untuk mengelola dan menganalisis untuk meminimalkan risiko yang akan diterima oleh perusahaan. Dengan demikian, kaitan antara keamanan sistem dan manajemen risiko adalah sebuah upaya yang dijalankan oleh pemangku kepentingan dalam organisasi dalam mengelola sebuah data dan informasi di sebuah organisasi dari sebuah risiko yang akan terjadi seperti peretasan sebuah data yang dilakukan oleh orang yang tidak ditanggung jawab.