Hasil dari tugas ini menghasilkan:

1. Dokumen IT Service level Management (Ms Words)
2. PPT melakukan presentasi untuk setiap kelompok ttg tugas ini
3. Perbaikan atau revisi dari setiap diskusi

Terima Kasih

Nama : M. Iqbal Rivana

IT Risk Management

21-Nov-2020

Universitas Bina Darma Palembang

1. **Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!**

Jawab : Bahwa pengelolaan IT saat ini menjadi lebih beragam bukan hanya sebatas pengelolaan security tetapi sudah menjadi lebih komplek, permasalahan kehidupan pribadi kemudian berbaur dengan suatu perusahaan/organisasi tertentu untuk itu perlu pemisahan antara sosial media antara kehidupan pribadi dan juga sosial media untuk kegiatan perusahaan atau organisasi, belakangan ini banyak pribadi-pribadi yang menjadikan sosial media nya sebagai alat untuk promosi dan juga alat komunikasi untuk perusahaan atau juga organisasi nya, sehingga menyebabkan bias nya isi dari media sosial dari pribadi tersebut, antara kehidupan pribadi nya dan juga kegiatan dari perusahaan atau organisasi.

2. **Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?**

Jawab : prinsip pemisahan tugas dimaksudkan untuk meminimalkan kesalahan dan mempersulit pemanfaatan hak akses untuk keuntungan pribadi, Separation of duties (SOD) adalah konsep kunci dari pengendalian internal dan merupakan yang paling sulit dan terkadang paling mahal untuk dicapai. Tujuan ini dicapai dengan menyebarkan tugas dan hak istimewa terkait untuk proses keamanan tertentu di antara banyak orang. SoD, yang berkaitan dengan keamanan, memiliki dua tujuan utama. Yang pertama adalah pencegahan konflik kepentingan (nyata atau nyata), tindakan yang salah, penipuan, penyalahgunaan dan kesalahan. Yang kedua adalah deteksi

kegagalan kontrol yang mencakup pelanggaran keamanan, pencurian informasi, dan pengelakan kontrol keamanan. SoD yang benar dirancang untuk memastikan bahwa individu tidak memiliki tanggung jawab yang saling bertentangan atau tidak bertanggung jawab untuk melaporkan diri mereka sendiri atau atasan mereka.

3. **Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!**

Jawab : **Privacy / Confidentiality:** Inti utama aspek pivacy atau confidentiality adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih ke arah data-data yang sifatnya privat, sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pedaftaran sebuah sevice) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Integrity: Aspek ini menentukan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dan sama persis seperti saat infomasi dikirimkan. Jika terdapat perbedaan antara infomasi atau data yang dikirimkan dengan yang diterima maka aspek integrity tidak tercapai. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin merupakan masalah yang harus dihadapi.

Berhubungan dengan akses untuk mengubah data dan informasi, data dan informasi yang berbeda dalam suatu sistem komputer hanya dapat diubah oleh orang berhak. Aspek ini menekankan bahwa informasi tidak boleh diubah tapa seizin pemilik infomasi. Adanya cirus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus dihadapi.

Authentication: Aspek ini berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengases atau memberikan informasi adalah betul-betul orang yang dimaksud, atau sever yang kita hubungi adalah betul-betul server yang asli. Biasanya metode yang sangat kita kenal untuk terkoneksi dengan server dan mendapatkan layanan adalah dengan metode password dimana terdapat suatu karakter yang diberikan oleh pengguna ke server dan server mengenalinya sesuai dengan policy yang ada. Saat ini dengan perkembangan TI

terdapat beberapa metode authentication yang lebih canggih dan aman seperti menggunakan retina mata, pengenalan suara, dan telapak tangan pengguna.

Availability: Aspek ini berhubungan dengan ketersediaan data dan informasi Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. Aspek availability atau keterseidaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Coba bayangkan jika kita sebagai user yang absah ingin mengakses mail atau layanan lainnya namun pada saat kita membutuhkannya layanan tersebut tidak dapat memenuhinya karena beberapa alasan, misalnya server yang down oleh serangan DoS, terkena Hack, atau terjadi Web Deface.

4. **Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!**

Jawab : IT risk management (manajemen resiko teknologi informasi) adalah proses yang dilakukan oleh para manajer IT untuk menyeimbangkan kegiatan operasional dan pengeluaran cost dalam mencapai keuntungan dengan melindungi sistem IT dan data yang medukung misi organisasinya. Menurut G. Stoneburner 2002, IT risk management meliputi tiga proses:

1. Risk Assessment

Penilaian resiko (risk assessment) merupakan proses awal di dalam metodologi manajemen resiko. Secara lebih spesifik sejak dikeluarkannya COSO Internal Control Integrated Framework, risk assessment dengan tegas dianggap sebagai salah satu komponen dari sistem internal control (Woods; 2007).

Organisasi menggunakan risk assessment untuk menentukan tingkat ancaman yang potensial dan resiko yang berhubungan dengan suatu sistem IT seluruh System Development Life Cycle (SDLC). Output hasil dari proses ini membantu kearah mengidentifikasi kendali yang sesuai untuk mengurangi atau menghapuskan resiko sepanjang/ketika proses peringanan resiko (risk mitigation). Untuk menentukan

kemungkinan suatu peristiwa/kejadian masa depan yang kurang baik, ancaman pada suatu sistem IT harus dianalisis bersama dengan vulnerability yang potensial dan pengendalian pada tempatnya untuk sistem IT. Menurut G. Stoneburner (2002) metodologi penilaian resiko meliputi sembilan langkah

2. Risk Mitigation

Risk mitigation adalah satu langkah yang melibatkan usaha-usaha untuk memprioritaskan, mengevaluasi dan menjalankan kontrol atau pengendalian yang dapat mengurangi resiko yang tepat yang direkomendasikan dari proses *risk assessment* (Stoneburner; 2002). *Risk mitigation* biasanya dilakukan dengan memenuhi pendekatan biaya terendah *(least-cost approach)* dan melaksanakan kontrol atau pengendalian yang paling tepat *(the most appropriate controls)* sehingga dapat mengurangi resiko ke dalam tingkat yang dapat diterima dengan resiko yang paling minim *(minimal adverse impact)* terhadap sumber daya dan tujuan organisasi.

3. Evaluation and assessment

Pada umumnya, di dalam suatu organisasi, jaringan secara terus menerus akan diperluas dan diperbaharui, komponen diubah dan aplikasi software-nya diganti atau diperbaharui dengan versi yang lebih baru. Perubahan ini berarti bahwa, resiko baru akan timbul dan resiko yang sebelumnya dikurangi, akan menjadi suatu perhatian. Demikian seterusnya, sehingga manajemen resiko akan berkembang.

Manajemen resiko seharusnya diselenggarakan dan terintergrasi dengan SDLC untuk sistem IT, bukan dikarenakan untuk kepentingan hukum atau regulasi, melainkan suatu “good practice” dan dukungan bisnis organisasi secara objektif atau berdasarkan misi.

5. **Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!**

Jawab : administrator keamanan teknologi informasi harus mengabdikan diri kira-kira sepertiga dari waktu mereka menangani aspek teknis. Yang tersisa dua pertiga harus digunakan untuk mengembangkan kebijakan dan prosedur, melakukan keamanan meninjau dan menganalisis risiko, menangani perencanaan kontingensi dan mempromosikan keamanan kesadaran;

- Keamanan lebih bergantung pada orang daripada pada teknologi;
- Karyawan adalah ancaman yang jauh lebih besar bagi keamanan informasi daripada orang luar;
- Keamanan itu seperti rantai. Itu sekuat mata rantai terlemahnya;
- Tingkat keamanan bergantung pada tiga faktor: risiko yang bersedia Anda ambil, fungsionalitas sistem dan biaya yang siap Anda bayarkan;
- Keamanan bukanlah status atau snapshot tetapi proses yang sedang berjalan.

Fakta-fakta ini pasti mengarah pada kesimpulan bahwa: Administrasi keamanan adalah manajemen dan BUKAN masalah teknis semata Oleh karena itu, pembentukan, pemeliharaan, dan pembaruan berkelanjutan dari ISMS menyediakan indikasi kuat bahwa perusahaan menggunakan pendekatan sistematis untuk identifikasi, penilaian dan manajemen risiko keamanan informasi. Selanjutnya perusahaan semacam itu akan mampu menangani kerahasiaan informasi, integritas dan persyaratan ketersediaan yang pada gilirannya berdampak pada:

- keberlangsungan bisnis;
- meminimalkan kerusakan dan kerugian;
- keunggulan kompetitif;
- profitabilitas dan arus kas;
- citra organisasi yang dihormati.

Tugas UTS IT Risk Management & Disaster Recovery

Nama : Nanda S. Prawira

NIM : 192420056

Soal:

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!
2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?
3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!
4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!
5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

Jawab :

1. Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:
   - Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.

- Melonjaknya biaya pengembangan sistem informasi karena adanya yang berlebihan.
- Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai.

Contohnya:

Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (*IT Governance*) (Herawan, 2012).

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (*Control Objectives for Information and Related Technology*) adalah standar internasional untuk tata kelola TIyang dikembangkan oleh ISACA (*Information System and Control Association*) dan ITGI (*IT Governance Institute*) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.(Wibowo, 2008).

2. Separation of Duties juga dikenal sebagai Pemisahan tugas, adalah konsep yang mengharuskan lebih dari satu orang untuk menyelesaikan suatu tugas. Ini adalah konsep kunci dari pengendalian internal dan merupakan yang paling sulit dan terkadang yang paling mahal untuk dicapai. Idenya adalah untuk menyebarkan tugas dan hak istimewa untuk tugas keamanan di antara banyak orang. Tidak ada orang yang harus melakukan segalanya.

Pemisahan tugas sudah terkenal dalam sistem akuntansi keuangan. Perusahaan dari semua ukuran memahami untuk tidak menggabungkan peran seperti menerima cek dan menyetujui penghapusan, menyetor uang tunai dan merekonsiliasi laporan bank, menyetujui kartu waktu dan memiliki hak asuh atas cek gaji, dan sebagainya.

Konsep Pemisahan tugas menjadi lebih relevan dengan organisasi TI ketika mandat regulasi seperti Sarbanes-Oxley (SOX) dan Gramm-Leach-Bliley Act (GLBA) diberlakukan. Porsi yang sangat tinggi dari masalah pengendalian internal SOX, misalnya, berasal dari atau bergantung pada TI. Ini memaksa organisasi TI untuk lebih menekankan pada Pemisahan tugas di semua fungsi TI, terutama keamanan.

Separation of Duties , karena berkaitan dengan keamanan, memiliki dua tujuan utama. Yang pertama adalah pencegahan konflik kepentingan (nyata atau nyata), tindakan yang salah, penipuan, penyalahgunaan dan kesalahan. Yang kedua adalah deteksi kegagalan kontrol yang mencakup pelanggaran keamanan, pencurian informasi, dan pengelakan kontrol keamanan.

Masalah Pemisahan tugas dalam keamanan terus menjadi signifikan. Sangat penting bahwa ada pemisahan antara operasi, pengembangan dan pengujian keamanan dan semua kontrol untuk mengurangi risiko aktivitas yang tidak sah atau akses ke sistem atau data operasional. Tanggung jawab harus diberikan kepada individu sedemikian rupa untuk mengamanatkan pemeriksaan dan keseimbangan dalam sistem dan meminimalkan peluang untuk akses tidak sah dan penipuan.

Ingat, teknik pengendalian seputar Pemisahan tugas dapat ditinjau oleh auditor eksternal. Auditor di masa lalu telah mencantumkan kekhawatiran ini sebagai kekurangan material pada laporan audit ketika mereka menentukan bahwa risikonya cukup besa

3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability :

a) ***Confidentiality***

Confidentiality merupakan aspek yang menjamin kerahasiaan data atau informasi. Sistem yang digunakan untuk mengimplementasikan e-procurement harus dapat menjamin kerahasiaan data yang dikirim, diterima dan disimpan. Bocornya informasi dapat berakibat batalnya proses pengadaan.

Kerahasiaan ini dapat diimplementasikan dengan berbagai cara, seperti misalnya menggunakan teknologi kriptografi dengan melakukan proses enkripsi (penyandian, pengkodean) pada transmisi data, pengolahan data (aplikasi dan database), dan penyimpanan data (storage). Teknologi kriptografi dapat mempersulit pembacaan data tersebut bagi pihak yang tidak berhak.

Seringkali perancang dan implementor dari sistem informasi atau sistem transaksi elektronik lalai dalam menerapkan pengamanan. Umumnya pengamanan ini baru diperhatikan pada tahap akhir saja sehingga pengamanan lebih sulit diintegrasikan dengan sistem yang ada. Penambahan pada tahap akhir ini menyebabkan sistem menjadi tambal sulam. Akibat lain dari hal ini adalah adanya biaya yang lebih mahal daripada jika pengamanan sudah dipikirkan dan diimplementasikan sejak awal.
Akses terhadap informasi juga harus dilakukan dengan melalui mekanisme otorisasi (*authorization*) yang ketat. Tingkat keamanan dari mekanisme otorisasi bergantung kepada tingkat kerahasiaan data yang diinginkan.

b) ***Integrity***
Integrity merupakan aspek yang menjamin bahwa data tidak boleh berubah tanpa ijin pihak yang berwenang (*authorized*). Untuk aplikasi e-procurement, aspek integrity ini sangat penting. Data yang telah dikirimkan tidak dapat diubah oleh pihak yang berwenang. Pelanggaran terhadap hal ini akan berakibat tidak berfungsinya sistem e-procurement.
Secara teknis ada banyak cara untuk menjamin aspek integrity ini, seperi misalnya dengan menggunakan *messange authentication code, hash function, digital signature*.

c) ***Availability***
Availability merupakan aspek yang menjamin bahwa data tersedia ketika dibutuhkan. Dapat dibayangkan efek yang terjadi ketika proses penawaran sedang dilangsungkan ternyata sistem tidak dapat diakses sehingga penawaran tidak dapat diterima. Ada kemungkinan pihak-pihak yang dirugikan karena tidak dapat mengirimkan penawaran, misalnya.
Hilangnya layanan dapat disebabkan oleh berbagai hal, mulai dari benca alam (kebakaran, banjir, gempa bumi), ke kesalahan sistem (server rusak, disk rusak, jaringan putus), sampai ke upaya pengrusakan yang dilakukan secara sadar (attack). Pengamanan terhadap ancaman ini dapat dilakukan dengan menggunakan sistem backup dan menyediakan *disaster recovery center* (DRC) yang dilengkapi dengan panduan untuk melakukan pemulihan (*disaster recovery plan*).

d) *Accountability*
Accountability artinya setiap kegiatan *user* di dalam jaringan akan direkam (*logged*) User tidak akan mencoba-coba untuk melanggar kebijakan keamanan karena identitas dan segala kegiatannya dapat dikenali sehingga mereka dapat dituntut secara hukum. Accountabilitymencehah illegal behavior. Di dalam sistem yang berbasis accountabilitymurni tidak diterapkan mekanisme *access control*.

4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka.

   Berdasarkan penjelasan tersebut, bisa dikatakan bahwa manajemen risiko dapat digunakan untuk meminimalisir dampak buruk yang timbul dari proses kerja di

perusahaan, tujuan dari manajemen risiko yang diterapkan di dalam perusahaan. Merujuk pada definisinya, salah satu tujuan yang pasti diinginkan oleh perusahaan adalah meminimalisir risiko yang timbul. Tujuannya yang pertama adalah untuk melindungi perusahaan. Sesuai dengan definisinya, poin ini merupakan tujuan utama dari manajemen risiko. Yakni dengan memberikan perlindungan terhadap perusahaan dari tingkat risiko signifikan yang bisa menghambat proses pencapaian tujuan perusahaan. Kemudian Membantu meningkatkan kinerja perusahaan juga menjadi salah satu tujuan dari manajemen risiko. Langkah nyatanya adalah dengan menyediakan informasi tingkat risiko yang disebutkan dalam peta risiko (*risk map*). Hal ini juga berguna dalam pengembangan strategi dan perbaikan proses *risk management* secara berkesinambungan. Selanjutnya untuk membangun kemampuan individu maupun manajemen perlu dilakukan sosialisasi tentang adanya risiko di dalam perusahaan. Untuk itulah diperlukan sosialisasi tentang tentang risiko dan pentingnya *risk management*.

5. Security administration is a management and NOT a purely technical issue yaitu suatu sistem untuk memberikan pemahaman yang utuh/ terpadu serta kemampuan dan keterampilan dalam merencanakan dan mendesain Sistem Pengamanan yang tepat, efektif, dan efisien, sesuai dengan situasi dan kondisi yang dihadapi, khususnya Ancaman / Gangguan yang mungkin terjadi serta kemampuan Perusahaan sendiri dan berguna untuk mencegah sedini mungkin kerugian-kerugian bagi Perusahaan. Kemudian dnegan management security administration bias memperkecil resiko kerusakan data dan kehilangan data karena sudah system sudah mempunyai alur yang didesain untuk keperluan administrasi.

TUGAS UJIAN TENGAH SEMESTER
IT RISK MANAGEMENT & DISASTER RECOVERY

NAMA : RAHMI

NIM : 192420046

SOAL !

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!
2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan anda jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?
3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!
4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!
5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

JAWABAN :

1. Yang di maksud dari pernyataan di atas yaitu, jika kehidupan pribadi di ikut sertakan dalam kehidupan perusaan maka akan beresiko terhadap kemajuan perusahaan, karena urusan pribadi tidak bias di ikutsertakan dalam urusan peruhaan, ini akan berdampak besar terhadap perusaan, dengan mencapuri urusan pribadi maka seorang tersebut tidak konsisten dalam pekerjaan, hal ini akan berdampak terhadap kemajuan proses pencapaian tujuan perusahaan.
   Contohnya, dampak konsistensi dalam bekerja. Kurangnya
2. Salah satu prinsip yang perlu di perhatikan dalam management resiko IT yaitu, prinsip pemisah tugas dimaksudkan untuk memonimasi sesalahan & mempersulit pengguna hak akses untuk keuntungan pribadi. Pemisah tugas sangat penting dalam system pengendalian internal, contohnya karyawan yang merancang system computer tidak boleh di tugaskan untuk pekerjaan yang menggunakan system tersebut, karena mereka bias saja merancang system yang menguntungkan mereka secara pribadi dan melakukan kecurangan.

3. Confidentiality merupakan aspek yang menjamin kerahasiaan data atau informasi. Sistem yang digunakan untuk mengimplementasikan e-procurement harus dapat menjamin kerahasiaan data yang dikirim, diterima dan disimpan. Bocornya informasi dapat berakibat batalnya proses pengadaan.

   Kerahasiaan ini dapat diimplementasikan dengan berbagai cara, seperti misalnya menggunakan teknologi kriptografi dengan melakukan proses enkripsi (penyandian, pengkodean) pada transmisi data, pengolahan data (aplikasi dan database), dan penyimpanan data (storage). Teknologi kriptografi dapat mempersulit pembacaan data tersebut bagi pihak yang tidak berhak. Seringkali perancang dan implementor dari sistem informasi atau sistem transaksi elektronik lalai dalam menerapkan pengamanan. Umumnya pengamanan ini baru diperhatikan pada tahap akhir saja sehingga pengamanan lebih sulit diintegrasikan dengan sistem yang ada. Penambahan pada tahap akhir ini menyebabkan sistem menjadi tambal sulam. Akibat lain dari hal ini adalah adanya biaya yang lebih mahal daripada jika pengamanan sudah dipikirkan dan diimplementasikan sejak awal.

   Akses terhadap informasi juga harus dilakukan dengan melalui mekanisme otorisasi (authorization) yang ketat. Tingkat keamanan dari mekanisme otorisasi bergantung kepada tingkat kerahasiaan data yang diinginkan.

   Accountability artinya setiap kegiatan user di dalam jaringan akan direkam (logged) User tidak akan mencoba-coba untuk melanggar kebijakan keamanan karena identitas dan segala kegiatannya dapat dikenali sehingga mereka dapat dituntut secara hukum. Accountabilitymencehah illegal behavior. Di dalam sistem yang berbasis accountabilitymurni tidak diterapkan mekanisme access control.
4. Maksud dari pernyataan di atas merupakan seorang manager di fungsikan untuk mengatur jalannya organisasi suatu perusahaan baik menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi. Management resiko adalah untuk mengurangi resiko yang berbeda beda yang berkitan dengan bidang yang telah dipilih pada tingkat yang dapat di terima dan di awasi oeh managernya. secara umum risiko dapat diartikan sebagai suatu keadaan yang dihadapi seseorang atau perusahaan dimana terdapat kemungkinan yang merugikan.
5. Berdasarkan penyataan di atas security management dapat melaksanakan prosedur system management kenyamanan dalam membentuk kerangka dasar bagi perusahaan agar dapat mengelola aspek keamanan dan ketertiban dengan mengatur dan mengendalikan potensi bahaya dan factor resiko guna mencapai perlindungan keamanan karyaran tamu dan masyarakat. Perlindungan mesin alat materi, dan harta benda perusahaan. Proses produksi yang aman handal, dan efisien, perlindungan yang berkualitas dan dapat di integrasikan dalam system management perusahaan yang ada dan menjadi bagian yang tidak dapat dipisahkan dari system management perusahaan secara keseluruhan.

TUGAS UJIAN TENGAH SEMESTER
IT RISK MANAGEMENT & DISASTER RECOVERY

NAMA : RANI OKTAFELANI

NIM : 192420048

SOAL !

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!
2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan anda jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?
3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!
4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!
5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

JAWABAN :

1. Yang di maksud dari pernyataan di atas yaitu, jika kehidupan pribadi di ikut sertakan dalam kehidupan perusaan maka akan beresiko terhadap kemajuan perusahaan, karena urusan pribadi tidak bias di ikutsertakan dalam urusan peruhaan, ini akan berdampak besar terhadap perusaan, dengan mencapuri urusan pribadi maka seorang tersebut tidak konsisten dalam pekerjaan, hal ini akan berdampak terhadap kemajuan proses pencapaian tujuan perusahaan.
   Contohnya, dampak konsistensi dalam bekerja. Kurangnya
2. Salah satu prinsip yang perlu di perhatikan dalam management resiko IT yaitu, prinsip pemisah tugas dimaksudkan untuk memonimasi sesalahan & mempersulit pengguna hak akses untuk keuntungan pribadi. Pemisah tugas sangat penting dalam system pengendalian internal, contohnya karyawan yang merancang system computer tidak boleh di tugaskan untuk pekerjaan yang menggunakan system tersebut, karena mereka bias saja merancang system yang menguntungkan mereka secara pribadi dan melakukan kecurangan.

3. Confidentiality merupakan aspek yang menjamin kerahasiaan data atau informasi. Sistem yang digunakan untuk mengimplementasikan e-procurement harus dapat menjamin kerahasiaan data yang dikirim, diterima dan disimpan. Bocornya informasi dapat berakibat batalnya proses pengadaan.

Kerahasiaan ini dapat diimplementasikan dengan berbagai cara, seperti misalnya menggunakan teknologi kriptografi dengan melakukan proses enkripsi (penyandian, pengkodean) pada transmisi data, pengolahan data (aplikasi dan database), dan penyimpanan data (storage). Teknologi kriptografi dapat mempersulit pembacaan data tersebut bagi pihak yang tidak berhak. Seringkali perancang dan implementor dari sistem informasi atau sistem transaksi elektronik lalai dalam menerapkan pengamanan. Umumnya pengamanan ini baru diperhatikan pada tahap akhir saja sehingga pengamanan lebih sulit diintegrasikan dengan sistem yang ada. Penambahan pada tahap akhir ini menyebabkan sistem menjadi tambal sulam. Akibat lain dari hal ini adalah adanya biaya yang lebih mahal daripada jika pengamanan sudah dipikirkan dan diimplementasikan sejak awal.

Akses terhadap informasi juga harus dilakukan dengan melalui mekanisme otorisasi (authorization) yang ketat. Tingkat keamanan dari mekanisme otorisasi bergantung kepada tingkat kerahasiaan data yang diinginkan.

Accountability artinya setiap kegiatan user di dalam jaringan akan direkam (logged) User tidak akan mencoba-coba untuk melanggar kebijakan keamanan karena identitas dan segala kegiatannya dapat dikenali sehingga mereka dapat dituntut secara hukum. Accountabilitymencehah illegal behavior. Di dalam sistem yang berbasis accountabilitymurni tidak diterapkan mekanisme access control.

4. Maksud dari pernyataan di atas merupakan seorang manager di fungsikan untuk mengatur jalannya organisasi suatu perusahaan baik menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi. Management resiko adalah untuk mengurangi resiko yang berbeda beda yang berkitan dengan bidang yang telah dipilih pada tingkat yang dapat di terima dan di awasi oeh managernya. secara umum risiko dapat diartikan sebagai suatu keadaan yang dihadapi seseorang atau perusahaan dimana terdapat kemungkinan yang merugikan.
5. Berdasarkan penyataan di atas security management dapat melaksanakan prosedur system management kenyamanan dalam membentuk kerangka dasar bagi perusahaan agar dapat mengelola aspek keamanan dan ketertiban dengan mengatur dan mengendalikan potensi bahaya dan factor resiko guna mencapai perlindungan keamanan karyaran tamu dan masyarakat. Perlindungan mesin alat materi, dan harta benda perusahaan. Proses produksi yang aman handal, dan efisien, perlindungan yang berkualitas dan dapat di integrasikan dalam system management perusahaan yang ada dan menjadi bagian yang tidak dapat dipisahkan dari system management perusahaan secara keseluruhan.

TUGAS UJIAN TENGAH SEMESTER
IT RISK MANAGEMENT & DISASTER RECOVERY

NAMA : SUWANI

NIM : 192420049

SOAL !

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!
2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan anda jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?
3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!
4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!
5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

JAWABAN :

1. Yang di maksud dari pernyataan di atas yaitu, jika kehidupan pribadi di ikut sertakan dalam kehidupan perusaan maka akan beresiko terhadap kemajuan perusahaan, karena urusan pribadi tidak bias di ikutsertakan dalam urusan peruhaan, ini akan berdampak besar terhadap perusaan, dengan mencapuri urusan pribadi maka seorang tersebut tidak konsisten dalam pekerjaan, hal ini akan berdampak terhadap kemajuan proses pencapaian tujuan perusahaan. Contohnya, dampak konsistensi dalam bekerja. Kurangnya
2. Salah satu prinsip yang perlu di perhatikan dalam management resiko IT yaitu, prinsip pemisah tugas dimaksudkan untuk memonimasi sesalahan & mempersulit pengguna hak akses untuk keuntungan pribadi. Pemisah tugas sangat penting dalam system pengendalian internal, contohnya karyawan yang merancang system computer tidak boleh di tugaskan untuk pekerjaan yang menggunakan system tersebut, karena mereka bias saja merancang system yang menguntungkan mereka secara pribadi dan melakukan kecurangan.

3. Confidentiality merupakan aspek yang menjamin kerahasiaan data atau informasi. Sistem yang digunakan untuk mengimplementasikan e-procurement harus dapat menjamin

kerahasiaan data yang dikirim, diterima dan disimpan. Bocornya informasi dapat berakibat batalnya proses pengadaan.

Kerahasiaan ini dapat diimplementasikan dengan berbagai cara, seperti misalnya menggunakan teknologi kriptografi dengan melakukan proses enkripsi (penyandian, pengkodean) pada transmisi data, pengolahan data (aplikasi dan database), dan penyimpanan data (storage). Teknologi kriptografi dapat mempersulit pembacaan data tersebut bagi pihak yang tidak berhak. Seringkali perancang dan implementor dari sistem informasi atau sistem transaksi elektronik lalai dalam menerapkan pengamanan. Umumnya pengamanan ini baru diperhatikan pada tahap akhir saja sehingga pengamanan lebih sulit diintegrasikan dengan sistem yang ada. Penambahan pada tahap akhir ini menyebabkan sistem menjadi tambal sulam. Akibat lain dari hal ini adalah adanya biaya yang lebih mahal daripada jika pengamanan sudah dipikirkan dan diimplementasikan sejak awal.

Akses terhadap informasi juga harus dilakukan dengan melalui mekanisme otorisasi (authorization) yang ketat. Tingkat keamanan dari mekanisme otorisasi bergantung kepada tingkat kerahasiaan data yang diinginkan.

Accountability artinya setiap kegiatan user di dalam jaringan akan direkam (logged) User tidak akan mencoba-coba untuk melanggar kebijakan keamanan karena identitas dan segala kegiatannya dapat dikenali sehingga mereka dapat dituntut secara hukum. Accountabilitymencehah illegal behavior. Di dalam sistem yang berbasis accountabilitymurni tidak diterapkan mekanisme access control.

4. Maksud dari pernyataan di atas merupakan seorang manager di fungsikan untuk mengatur jalannya organisasi suatu perusahaan baik menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi. Management resiko adalah untuk mengurangi resiko yang berbeda beda yang berkitan dengan bidang yang telah dipilih pada tingkat yang dapat di terima dan di awasi oeh managernya. secara umum risiko dapat diartikan sebagai suatu keadaan yang dihadapi seseorang atau perusahaan dimana terdapat kemungkinan yang merugikan.
5. Berdasarkan penyataan di atas security management dapat melaksanakan prosedur system management kenyamanan dalam membentuk kerangka dasar bagi perusahaan agar dapat mengelola aspek keamanan dan ketertiban dengan mengatur dan mengendalikan potensi bahaya dan factor resiko guna mencapai perlindungan keamanan karyaran tamu dan masyarakat. Perlindungan mesin alat materi, dan harta benda perusahaan. Proses produksi yang aman handal, dan efisien, perlindungan yang berkualitas dan dapat di integrasikan dalam system management perusahaan yang ada dan menjadi bagian yang tidak dapat dipisahkan dari system management perusahaan secara keseluruhan.

Nama : Theo Vhaldino
Nim : 192420058
Angkatan/Reguler : 22 / A R1
Mata Kuliah : IT RISK MANAGEMENT & DISASTER RECOVERY (MTIK232)

UJIAN TENGAH SEMESTER

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!

   Penyelesaian :

   Dalam kehidupan sehari-hari, istilah risiko mungkin bukan hal yang baru dalam kehidupan kita. Risiko biasanya berkaitan dengan sesuatu yang tidak diinginkan, hal-hal yang harus dihindari, dan identik dengan suatu ketidakpastian. Begitu juga dalam aktivitas organisasi, segala aktivitas program yang telah direncanakan memiliki berbagai tingkat risiko.

   Namun, faktanya banyak lembaga atau organisasi sering mengabaikan pentingnya manajemen risiko karena terlalu terfokus pada tujuan program. Adanya risiko pada aktivitas program harus dapat diantisipasi dengan melakukan pendekatan melalui proses identifikasi, analisis, dan pengelolaan konsekuensi oleh organisasi. Pengelolaan risiko menjadi bagian yang penting karena suatu organisasi harus mampu untuk mengambil risiko dengan tepat. Oleh karena itu, manajemen risiko (*risk management*) perlu untuk dipahami.

   Salah satu contoh di kehidupan sehari-hari Semisal ketika kita begadang dimalam hari, banyak risiko yang akan terjadi sesudahnya, seperti telat bangun, badan lelah, dan Banyak hal yang akan terjadi. Salah satu pencegahannya ialah minum kopi agar tidak mengantuk. Secara bahasa manajemen risiko adalah upaya untuk mengurangi dampak dari unsur ketidakpastian, sehingga minum kopi dapat dikatakan sebagai manajemen risiko pada begadang di malam hari.

   Secara sederhana Manajemen Risiko adalah pengelolaan risiko, yang terdiri dari 4 kegiatan, yaitu mengidentifikasi risiko, mengukur dampak dan

frekuensinya, memitigasi (mencari solusi untuk mencegahnya atau mengantisipasinya) dan monitoring.

2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?

   Penyelesaian :

   Pemisahan tugas sangat penting dalam sistem pengendalian internal karena mengurangi risiko kesalahan dan tindakan tidak pantas. Ini membantu melawan penipuan oleh mengecilkan kolusi.

   Contohnya, karyawan yang merancang sistem komputer tidak boleh ditugaskan untuk pekerjaan yang menggunakan sistem tersebut, kaerena mereka bisa saja merancang sistem yang menguntungkan mereka secara pribadi dan melakukan kecurangan. Adapun Bagian penting dalam keamanan IT pada pemisahan tugas, antara lain :

   1. Bagian pengontrol data
   2. Bagian yang mempersiapkan data
   3. Bagian operasi komputer
   4. Bagian pustaka data
   5. Bagian pemrogram dan pengembangan sistem, dan
   6. Bagian pusat informasi (information center)

3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!

   Penyelesaian :

   1) ***Confidentiality*** merupakan aspek yang menjamin kerahasiaan data atau informasi. Sistem yang digunakan untuk mengimplementasikan e-procurement harus dapat menjamin kerahasiaan data yang dikirim, diterima dan disimpan. Bocornya informasi dapat berakibat batalnya proses pengadaan. Kerahasiaan ini dapat diimplementasikan dengan berbagai cara, seperti misalnya menggunakan teknologi kriptografi dengan melakukan proses enkripsi (penyandian, pengkodean) pada transmisi data, pengolahan data (aplikasi dan database), dan penyimpanan data (storage). Teknologi kriptografi dapat mempersulit pembacaan data tersebut bagi pihak yang tidak berhak. Seringkali perancang dan implementor dari sistem informasi atau

sistem transaksi elektronik lalai dalam menerapkan pengamanan. Umumnya pengamanan ini baru diperhatikan pada tahap akhir saja sehingga pengamanan lebih sulit diintegrasikan dengan sistem yang ada. Penambahan pada tahap akhir ini menyebabkan sistem menjadi tambal sulam. Akibat lain dari hal ini adalah adanya biaya yang lebih mahal daripada jika pengamanan sudah dipikirkan dan diimplementasikan sejak awal. Akses terhadap informasi juga harus dilakukan dengan melalui mekanisme otorisasi (authorization) yang ketat. Tingkat keamanan dari mekanisme otorisasi bergantung kepada tingkat kerahasiaan data yang diinginkan.

2) ***Integrity*** merupakan aspek yang menjamin bahwa data tidak boleh berubah tanpa ijin pihak yang berwenang (authorized). Untuk aplikasi e-procurement, aspek integrity ini sangat penting. Data yang telah dikirimkan tidak dapat diubah oleh pihak yang berwenang. Pelanggaran terhadap hal ini akan berakibat tidak berfungsinya sistem e-procurement. Secara teknis ada banyak cara untuk menjamin aspek integrity ini, seperi misalnya dengan menggunakan messange authentication code, hash function, digital signature.
3) ***Availability*** merupakan aspek yang menjamin bahwa data tersedia ketika dibutuhkan. Dapat dibayangkan efek yang terjadi ketika proses penawaran sedang dilangsungkan ternyata sistem tidak dapat diakses sehingga penawaran tidak dapat diterima. Ada kemungkinan pihak-pihak yang dirugikan karena tidak dapat mengirimkan penawaran, misalnya. Hilangnya layanan dapat disebabkan oleh berbagai hal, mulai dari benca alam (kebakaran, banjir, gempa bumi), ke kesalahan sistem (server rusak, disk rusak, jaringan putus), sampai ke upaya pengrusakan yang dilakukan secara sadar (attack). Pengamanan terhadap ancaman ini dapat dilakukan dengan menggunakan sistem backup dan menyediakan disaster recovery center (DRC) yang dilengkapi dengan panduan untuk melakukan pemulihan (disaster recovery plan).
4) ***Accountability*** artinya setiap kegiatan user di dalam jaringan akan direkam (logged) User tidak akan mencoba-coba untuk melanggar kebijakan keamanan karena identitas dan segala kegiatannya dapat dikenali sehingga mereka dapat dituntut secara hukum. Accountability mencegah illegal behavior. Di dalam sistem yang berbasis accountability murni tidak diterapkan mekanisme access control.

4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!

   Penyelesaian :

   Adanya peran manajemen resiko dalam suatu organisasi diharapkan dapat menuntun suatu organisasi untuk perjalanan ke depannya (*forward-looking*). Hal ini dikarenakan yang namanya strategi tidak bisa langsung diterapkan secara pasti di dalam perjalanan organisasi karena harus disesuaikan dengan perkembangan situasi organisasi tersebut. Dengan demikian, manajemen risiko dapat membantu suatu organisasi dalam menetapkan strategi ke depannya, kemudian meninjau kembali strategi yang telah diterapkan sehingga dapat relevan dengan situasi yang terus berkembang.

   Beberapa manfaat dari penerapan manajemen risiko yang efisien dalam program organisasi, diantaranya:

   1) Memberikan hasil program yang lebih baik karena melalui pengambilan keputusan yang tepat.
   2) Mengakui adanya ketidakpastian/risiko dengan memberikan perkiraan pada hasil yang mungkin terjadi.
   3) Menekan biaya untuk penanggulangan kejadian yang tidak diharapkan.
   4) Menciptakan rasa aman dan meningkatkan pemahaman dan kesadaran pelaku program mengenai risiko yang mungkin dihadapi.

   Dengan penerapan manajemen risiko secara terstruktur dan terintegrasi, organisasi akan mampu beradaptasi dengan memahami kondisi lingkungan sekitar sekaligus dapat memberikan kebijakan yang tepat untuk mencapai tujuan program.

5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

   Penyelesaian :

   Security Administration tidak selalu dikaitkan dengan technical issue. Manajemen sangat berpengaruh dan penting diterapkan agar informasi yang beredar di perusahaan atau di organisasi dapat dikelola dengan benar sehingga

perusahaan / organisasi dapat mengambil keputusan berdasarkan informasi yang ada dengan benar pula dalam rangka memberikan layanan yang terbaik.dalam manajemen keamanan informasi terdiri dari empat langkah :

1) Identifikasi threats (ancaman) yang dapat menyerang sumber daya informasi perusahaan
2) Mendefinisikan resiko dari ancaman yang dapat memaksakan
3) Penetapan kebijakan keamanan informasi
4) Menerapkan controls yang tertuju pada resiko

Dengan kesimpulan, bahwa pada dasarnya manajemen sangat membantu dan memberikan solusi terhadap *Security Administration* bukan hanya sekedar masalah teknis saja, melainkan pengelolaan yang tepat guna.

Mata Kuliah : IT RISK MANAGEMENT & DISASTER RECOVERY (MTIK232)
Tugas : Ujian TEngah Semester
Nama : Yayan Candra Subidin
NIM : 192420054

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!

   Tanggapan :

   Teknologi kini telah menjadi kebutuhan dalam kehidupan sehari-hari, termasuk dalam operasional perusahaan. Penggabungan antara komputer dengan telekomunikasi telah menghasilkan suatu revolusi di bidang sistem informasi, di mana teknologi sangat berperan di dalam meningkatkan produktivitas perusahaan. Meski penggunaan teknologi dalam perusahaan dapat meningkatkan efisiensi dan meminimalisir biaya, namun kemajuan teknologi juga memiliki dampak yang tidak baik. Di antaranya adalah:

   - Kemajuan teknologi akan membuat perusahaan lebih mengutamakan penggunaan teknologi dibandingkan dengan sumber daya manusia. Sehingga penggunaan sumber daya manusia akan semakin berkurang.
   - Kemajuan teknologi akan membuat perusahaan lebih mengutamakan pekerjaan pada *core business*. Sehingga aktivitas lainnya lebih cenderung mempergunakan karyawan dengan sistem kontrak atau paruh waktu.
   - Hubungan kontak langsung antara pelanggan dengan manajemen di perusahaan akan semakin sulit dibina. Karena lokasi kegiatan tidak lagi terpusat pada satu tempat saja, tetapi menyebar ke tempat lainnya. Karena dengan menggunakan email, telepon dan lainnya, maka para manajemen dapat berhubungan dengan pelanggan. Tanpa harus bertemu secara langsung, sehingga hubungan relasi yang dekat akan semakin berkurang.

2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?

   Tanggapan :

   Prinsip Separation of Duties sangat perlu dalam mengelola resiko IT agar tidak terjadi hal-hal yang yang tidak diinginkan dalam pengelolaan IT seperti seperti penyalah gunaan kode-kode atau data yang curang atau berbahaya tanpa terdeteksi. Kontrol yang ketat atas perangkat IT dan perubahan data akan mengharuskan orang atau organisasi yang sama melakukan hanya satu dari peran berikut:

   - Identifikasi persyaratan (atau permintaan perubahan); misalnya seorang pebisnis
   - Otorisasi dan persetujuan; misalnya, dewan atau manajer tata kelola TI
   - Perancangan dan pengembangan; misalnya seorang pengembang
   - Review, inspeksi dan persetujuan ; misal pengembang atau arsitek lain.
   - Implementasi dalam produksi; biasanya perubahan perangkat lunak atau administrator sistem .

Untuk berhasil menerapkan pemisahan tugas dalam sistem informasi, sejumlah masalah perlu diperhatikan:

- Proses yang digunakan untuk memastikan hak otorisasi seseorang dalam sistem sejalan dengan perannya dalam organisasi.
- Metode otentikasi yang digunakan seperti pengetahuan tentang kata sandi, kepemilikan objek (kunci, token) atau karakteristik biometrik.
- Pengelakan hak dalam sistem dapat terjadi melalui akses administrasi database, akses administrasi pengguna, alat yang menyediakan akses pintu belakang atau akun pengguna yang dipasang oleh pemasok. Kontrol khusus seperti tinjauan log aktivitas mungkin diperlukan untuk menangani masalah khusus ini.

3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!
   Tanggapan :

   Konsep Network Security
   Dalam menjaga kemanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut dengan CIA yang merupakan; *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan).

   Confidentiality adalah seperangkat aturan yang membatasi akses ke informasi. *Integrity* adalah jaminan bahwa informasi itu dapat dipercaya dan akurat, serta *Availability* yang merupakan konsep dimana informasi tersebut selalu tersedia ketika dibutuhkan oleh orang-orang yang memiliki akses atau wewenang.

   1*. Confidentiality* (kerahasiaan)
   Kerahasiaan setara dengan privasi. Kerahasiaan dirancang untuk mencegah informasi sensitif dan memastikan bahwa orang yang mempunyai akses adalah orang yang tepat. Terkadang menjaga kerahasiaan data dapat melibatkan pelatihan khusus bagi mereka yang mengetahui dokumen tersebut.

   2. *Integrity* (integritas)
   Integritas melibatkan menjaga konsistensi, akurasi, dan kepercayaan data. Data tidak boleh diubah, dan langkah-langkah harus diambil untuk memastikan bahwa data tidak dapat diubah oleh orang-orang yang tidak berkepentingan.

   3. *Availability* (ketersediaan)
   Ketersediaan (*availability*) adalah konsep terbaik yang dapat dipastikan dalam memelihara semua *hardware*, melakukan perbaikan terhadap *hardware* sesegera mungkin saat diperlukan. Selain itu juga dapat memelihara lingkungan sistem operasi.

4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!

   Tanggapan :

   Manajer TI tidak hanya berfokus tentang penanganan terhadap risiko dan dampak negative dari hambatan-hambatan di atas terhadap operasional perusahaan dalam hal value sebuah perusahaan, tetapi juga dapat memberikan keuntungan potensial maka manajer IT dapat Mengelola risiko teknologi informasi dalam sebuah perusahaan sebagai berikut :

   a. *Assessment*, merujuk pada pencarian risiko dan penilaian tingkat keparahan risiko.
   b. *Mitigation*, yaitu penanggulanan yang dilakukan untuk mengurangi dampat risiko.
   c. *Evaluation and Assessment*, merujuk pada evaluasi terhadap penanggulangan yang sudah dilakukan.

5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

   Tanggapan :

   Keamanan informasi tidak hanya tergantung pada teknis saja tetapi diperlukan kebijakan atau regulasi yang tepat dalam menciptakan keamanan informasi.

Mata Kuliah : IT RISK MANAGEMENT & DISASTER RECOVERY (MTIK232)
Tugas : Ujian TEngah Semester
Nama : Yayan Candra Subidin
NIM : 192420054

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!

   Tanggapan :

   Teknologi kini telah menjadi kebutuhan dalam kehidupan sehari-hari, termasuk dalam operasional perusahaan. Penggabungan antara komputer dengan telekomunikasi telah menghasilkan suatu revolusi di bidang sistem informasi, di mana teknologi sangat berperan di dalam meningkatkan produktivitas perusahaan. Meski penggunaan teknologi dalam perusahaan dapat meningkatkan efisiensi dan meminimalisir biaya, namun kemajuan teknologi juga memiliki dampak yang tidak baik. Di antaranya adalah:

   - Kemajuan teknologi akan membuat perusahaan lebih mengutamakan penggunaan teknologi dibandingkan dengan sumber daya manusia. Sehingga penggunaan sumber daya manusia akan semakin berkurang.
   - Kemajuan teknologi akan membuat perusahaan lebih mengutamakan pekerjaan pada *core business*. Sehingga aktivitas lainnya lebih cenderung mempergunakan karyawan dengan sistem kontrak atau paruh waktu.
   - Hubungan kontak langsung antara pelanggan dengan manajemen di perusahaan akan semakin sulit dibina. Karena lokasi kegiatan tidak lagi terpusat pada satu tempat saja, tetapi menyebar ke tempat lainnya. Karena dengan menggunakan email, telepon dan lainnya, maka para manajemen dapat berhubungan dengan pelanggan. Tanpa harus bertemu secara langsung, sehingga hubungan relasi yang dekat akan semakin berkurang.

2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?

   Tanggapan :

   Prinsip Separation of Duties sangat perlu dalam mengelola resiko IT agar tidak terjadi hal-hal yang yang tidak diinginkan dalam pengelolaan IT seperti seperti penyalah gunaan kode-kode atau data yang curang atau berbahaya tanpa terdeteksi. Kontrol yang ketat atas perangkat IT dan perubahan data akan mengharuskan orang atau organisasi yang sama melakukan hanya satu dari peran berikut:

   - Identifikasi persyaratan (atau permintaan perubahan); misalnya seorang pebisnis
   - Otorisasi dan persetujuan; misalnya, dewan atau manajer tata kelola TI
   - Perancangan dan pengembangan; misalnya seorang pengembang
   - Review, inspeksi dan persetujuan ; misal pengembang atau arsitek lain.
   - Implementasi dalam produksi; biasanya perubahan perangkat lunak atau administrator sistem .

Untuk berhasil menerapkan pemisahan tugas dalam sistem informasi, sejumlah masalah perlu diperhatikan:

- Proses yang digunakan untuk memastikan hak otorisasi seseorang dalam sistem sejalan dengan perannya dalam organisasi.
- Metode otentikasi yang digunakan seperti pengetahuan tentang kata sandi, kepemilikan objek (kunci, token) atau karakteristik biometrik.
- Pengelakan hak dalam sistem dapat terjadi melalui akses administrasi database, akses administrasi pengguna, alat yang menyediakan akses pintu belakang atau akun pengguna yang dipasang oleh pemasok. Kontrol khusus seperti tinjauan log aktivitas mungkin diperlukan untuk menangani masalah khusus ini.

3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!
   Tanggapan :

   Konsep Network Security
   Dalam menjaga kemanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut dengan CIA yang merupakan; *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan).

   Confidentiality adalah seperangkat aturan yang membatasi akses ke informasi. *Integrity* adalah jaminan bahwa informasi itu dapat dipercaya dan akurat, serta *Availability* yang merupakan konsep dimana informasi tersebut selalu tersedia ketika dibutuhkan oleh orang-orang yang memiliki akses atau wewenang.

   1*. Confidentiality* (kerahasiaan)
   Kerahasiaan setara dengan privasi. Kerahasiaan dirancang untuk mencegah informasi sensitif dan memastikan bahwa orang yang mempunyai akses adalah orang yang tepat. Terkadang menjaga kerahasiaan data dapat melibatkan pelatihan khusus bagi mereka yang mengetahui dokumen tersebut.

   2. *Integrity* (integritas)
   Integritas melibatkan menjaga konsistensi, akurasi, dan kepercayaan data. Data tidak boleh diubah, dan langkah-langkah harus diambil untuk memastikan bahwa data tidak dapat diubah oleh orang-orang yang tidak berkepentingan.

   3. *Availability* (ketersediaan)
   Ketersediaan (*availability*) adalah konsep terbaik yang dapat dipastikan dalam memelihara semua *hardware*, melakukan perbaikan terhadap *hardware* sesegera mungkin saat diperlukan. Selain itu juga dapat memelihara lingkungan sistem operasi.

4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!

   Tanggapan :

   Manajer TI tidak hanya berfokus tentang penanganan terhadap risiko dan dampak negative dari hambatan-hambatan di atas terhadap operasional perusahaan dalam hal value sebuah perusahaan, tetapi juga dapat memberikan keuntungan potensial maka manajer IT dapat Mengelola risiko teknologi informasi dalam sebuah perusahaan sebagai berikut :

   a. *Assessment*, merujuk pada pencarian risiko dan penilaian tingkat keparahan risiko.
   b. *Mitigation*, yaitu penanggulanan yang dilakukan untuk mengurangi dampat risiko.
   c. *Evaluation and Assessment*, merujuk pada evaluasi terhadap penanggulangan yang sudah dilakukan.

5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

   Tanggapan :

   Keamanan informasi tidak hanya tergantung pada teknis saja tetapi diperlukan kebijakan atau regulasi yang tepat dalam menciptakan keamanan informasi.

Mata Kuliah :
Tugas : Ujian Tengah Semester
Nama : Al Adri Nofa Gusandi
NIM : 192420053

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda ?

   Tanggapan :

   Teknologi kini telah menjadi kebutuhan dalam kehidupan sehari-hari, termasuk dalam operasional perusahaan. Penggabungan antara komputer dengan telekomunikasi telah menghasilkan suatu revolusi di bidang sistem informasi, di mana teknologi sangat berperan di dalam meningkatkan produktivitas perusahaan. Meski penggunaan teknologi dalam perusahaan dapat meningkatkan efisiensi dan meminimalisir biaya, namun kemajuan teknologi juga memiliki dampak yang tidak baik. Di antaranya adalah:

   - Kemajuan teknologi akan membuat perusahaan lebih mengutamakan penggunaan teknologi dibandingkan dengan sumber daya manusia. Sehingga penggunaan sumber daya manusia akan semakin berkurang.
   - Kemajuan teknologi akan membuat perusahaan lebih mengutamakan pekerjaan pada *core business*. Sehingga aktivitas lainnya lebih cenderung mempergunakan karyawan dengan sistem kontrak atau paruh waktu.
   - Hubungan kontak langsung antara pelanggan dengan manajemen di perusahaan akan semakin sulit dibina. Karena lokasi kegiatan tidak lagi terpusat pada satu tempat saja, tetapi menyebar ke tempat lainnya. Karena dengan menggunakan email, telepon dan lainnya, maka para manajemen dapat berhubungan dengan pelanggan. Tanpa harus bertemu secara langsung, sehingga hubungan relasi yang dekat akan semakin berkurang.

2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT ?

   Tanggapan :

   Prinsip Separation of Duties sangat perlu dalam mengelola resiko IT agar tidak terjadi hal-hal yang yang tidak diinginkan dalam pengelolaan IT seperti seperti penyalah gunaan kode-kode atau data yang curang atau berbahaya tanpa terdeteksi. Kontrol yang ketat atas perangkat IT dan perubahan data akan mengharuskan orang atau organisasi yang sama melakukan hanya satu dari peran berikut:

   - Identifikasi persyaratan (atau permintaan perubahan); misalnya seorang pebisnis
   - Otorisasi dan persetujuan; misalnya, dewan atau manajer tata kelola TI
   - Perancangan dan pengembangan; misalnya seorang pengembang
   - Review, inspeksi dan persetujuan ; misal pengembang atau arsitek lain.

- ❖ Implementasi dalam produksi; biasanya perubahan perangkat lunak atau administrator sistem .

Untuk berhasil menerapkan pemisahan tugas dalam sistem informasi, sejumlah masalah perlu diperhatikan:

- ❖ Proses yang digunakan untuk memastikan hak otorisasi seseorang dalam sistem sejalan dengan perannya dalam organisasi.
- ❖ Metode otentikasi yang digunakan seperti pengetahuan tentang kata sandi, kepemilikan objek (kunci, token) atau karakteristik biometrik.
- ❖ Pengelakan hak dalam sistem dapat terjadi melalui akses administrasi database, akses administrasi pengguna, alat yang menyediakan akses pintu belakang atau akun pengguna yang dipasang oleh pemasok. Kontrol khusus seperti tinjauan log aktivitas mungkin diperlukan untuk menangani masalah khusus ini.

3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda?

Tanggapan :

Konsep Network Security

Dalam menjaga kemanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut dengan CIA yang merupakan; *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan).

Confidentiality adalah seperangkat aturan yang membatasi akses ke informasi. *Integrity* adalah jaminan bahwa informasi itu dapat dipercaya dan akurat, serta *Availability* yang merupakan konsep dimana informasi tersebut selalu tersedia ketika dibutuhkan oleh orang-orang yang memiliki akses atau wewenang.

1. *Confidentiality* (kerahasiaan)

Kerahasiaan setara dengan privasi. Kerahasiaan dirancang untuk mencegah informasi sensitif dan memastikan bahwa orang yang mempunyai akses adalah orang yang tepat. Terkadang menjaga kerahasiaan data dapat melibatkan pelatihan khusus bagi mereka yang mengetahui dokumen tersebut.

2. *Integrity* (integritas)

Integritas melibatkan menjaga konsistensi, akurasi, dan kepercayaan data. Data tidak boleh diubah, dan langkah-langkah harus diambil untuk memastikan bahwa data tidak dapat diubah oleh orang-orang yang tidak berkepentingan.

3. *Availability* (ketersediaan)

Ketersediaan (*availability*) adalah konsep terbaik yang dapat dipastikan dalam memelihara semua *hardware*, melakukan perbaikan terhadap *hardware* sesegera mungkin saat diperlukan. Selain itu juga dapat memelihara lingkungan sistem operasi.

4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data

yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini?

Tanggapan :

Manajer TI tidak hanya berfokus tentang penanganan terhadap risiko dan dampak negative dari hamatan-hambatan di atas terhadap operasional perusahaan dalam hal value sebuah perusahaan, tetapi juga dapat memberikan keuntungan potensial maka manajer IT dapat Mengelola risiko teknologi informasi dalam sebuah perusahaan sebagai berikut :

a. ***Assessment***, merujuk pada pencarian risiko dan penilaian tingkat keparahan risiko.
b. ***Mitigation***, yaitu penanggulanan yang dilakukan untuk mengurangi dampat risiko.
c. ***Evaluation and Assessment***, merujuk pada evaluasi terhadap penanggulangan yang sudah dilakukan.

5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut ?

Tanggapan :

Keamanan informasi tidak hanya tergantung pada teknis saja tetapi diperlukan kebijakan atau regulasi yang tepat dalam menciptakan keamanan informasi.

Nama : Arpa Pauziah

NIM : 192420055

Mata Kuliah : IT Risk Management & Disaster Recovery

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!
2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?
3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!
4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!
5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

JAWABAN:

1. “pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi” maksud daripernyataan tersebut adalah seseorang bisa menggunakan data dirinya untuk dijadikan password. Contohnya tanggal lahir.
2. Di dalam sistem informasi yang sangat terintegrasi, prosedur yang dahulu dilakukan oleh beberapa orang, kini digabungkan. Oleh sebab itu, siapapun yang memiliki akses tak terbatas ke komputer, program komputer, dan data, dapat memiliki kesempatan untuk melakukan kejahatan dan menyembunyikan penipuan. Dalam rangka memerangi ancaman ini, organisasi harus

mengimplementasikan prosedur pengendalian yang sesuai, seperti pemisahan tugas yang efektif dalam fungsi sistem informasi.

Merupakan hal yang penting untuk diketahui bahwa orang-orang yang melakukan fungsi¬-fungsi ini haruslah orang-orang yang berbeda. Mengizinkan seseorang untuk melakukan dua atau lebih pekerjaan, akan menghadapkan perusahaan pada kemungkinan terjadinya penipuan.

Contohnya, apabila seorang programer untuk sebuah lembaga pemberi kredit diizinkan untuk menggunakan data asli dalam menguji program yang dibuatnya, maka dia dapat menghapus saldo kredit mobilnya ketika melaksanakan uji tersebut. Seperti juga halnya apabila seorang operator komputer memiliki akses ke logika program dan dokumentasinya, dia bisa saja, ketika memproses program penggajian perusahaan, mengubah program untuk menaikkan gajinya.

Sebagai tambahan atas pemisahan tugas yang memadai, organisasi harus memastikan bahwa orang yang mendesain, mengembangkan, mengimplementasikan, dan mengoperasikan sistem informasi milik perusahaan, berkualifikasi serta terlatih baik. Kondisi yang sama juga harus diberlakukan bagi orang-orang yang bertanggung jawab atas pengamanan sistem.

3. Keamanan Sistem Informasi dimaksudkan untuk mecapai tiga sasaran utama sebagai berikut :

   - ***Kerahasiaan (Confidentiality)*** Membutuhkan bahwa informasi (data) hanya bisa diakses oleh mereka yang memiliki otoritas.
   - ***Integritas (Integrity)*** Membutuhkan bahwaa informasi hanya dapat diubah oleh pihak yang memiliki otoritas.
   - ***Ketersediaan (Availability)*** Mensyaratkan bahwa ketersediaan informasi yang tersedia bagi mereka yang memiliki wewenang ketika dibutuhkan.

4. Kepala unit organisasi harus memastikan bahwa organisasi memiliki kemampuan yang dibutuhkan untuk menyelesaikan misinya. Pemilik misi ini harus menentukan kemampuan keamanan yang harus dimiliki oleh sistem TI mereka untuk memberikan tingkat dukungan misi yang diinginkan dalam menghadapi ancaman dunia nyata. Sebagian besar organisasi memiliki anggaran yang ketat untuk keamanan TI; oleh karena itu, pengeluaran keamanan TI harus

ditinjau selengkap keputusan manajemen lainnya. Metodologi manajemen risiko yang terstruktur dengan baik, bila digunakan secara efektif, dapat membantu manajemen mengidentifikasi kontrol yang sesuai untuk menyediakan kemampuan keamanan yang penting bagi misi.

5. Security administration is a management and NOT a purely technical issue

   Maksudnya adalah Banyak organisasi yang memanfaatkan perangkat teknologi informasi berbasis jaringan baik local maupun global untuk mendukung tujuan pengembangan organisasinya. Namun banyak yang tanpa disadari mengimplementasikan sistem jaringan computer tersebut tanpa dibarengi dan diimbangi dengan sistem keamanan yang memadai sesuai dengan standar keamanan yang berlaku. Hal itu dikarenakan karena banyak yang tidak menggunakan prinsip-prinsip pengamanan sesuai standar, dan dalam mengimplementasikan tidak melalui tahap siklus hidup keamanan informasi.

NAMA **: ELPINA SARI**

NIM **: 192420050**

UTS **: IT RISK MANAGEMENT**

SOAL

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!
2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?
3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!
4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!
5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

JAWABAN:

1. Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan. Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain yaitu Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi, Melonjaknya biaya pengembangan sistem informasi karena adanya "scope creep" (atau pengembangan berlebihan) yang tanpa terkendali dan Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi.

   Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Contohnya adalah Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri. Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI. Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi.

2. Prinsip keamanan IT Separation of duties perlu di perhatikan dalam manajemen resiko IT bertujuan untuk memastikan bahwa tidak satu orang karyawan pun yang mengendalikan sebuah transaksi dari awal sampai akhir, dua atau lebih orang harus bertanggung jawab untuk melakukannya. Contohnya adalah bahwa siapapun yang diperbolehkan untuk membuat sebuah transaksi tidak dapat dimanipulasi untuk kepentingan pribadi, kecuali seluruh orang yang terlibat didalamnya terlibat

3. CIAA (Confidential, Integrity, Availability dan Accountability)

- Confidential

  Konsep ini mencegah pengungkapan informasi untuk orang yang tidak berhak. Menjamin data, informasi, objek dan sumberdaya terbatas dari subjek yang tidak ter-otorisasi. Setiap data penting harus terjaga kerahasiaannya. Tidak benar jika semua informasi boleh diakses oleh semua orang, harus dibagi sesuai dengan kepentingannya, kecuali informasi tersebut sifatnya umum setiap orang boleh tau/akses.

  Contohnya : jika teman-teman memiliki access point wifi di rumah, lalu tetangga dapat dengan mudah tanpa password untuk menggunakan access point wifi teman-teman, maka dalam hal ini konsep Confidentialitynya menjadi rendah/hilang.

  Jenis ancaman serangan pada prinsip security ini meliputi mengintip lalu lintas network(biasanya dilakukan di access point wifi public di café atau tempat makan), mencuri password menggunakan social engineering, melakukan port scanning pada server, dan banyak aktifitas lainnya yang berusaha untuk mengambil data atau informasi penting.

  Jika ada ancaman, tentu saja ada langkah pencegahannya, yaitu dengan menerapkan enkripsi pada informasi penting, penerapan akses control yang ketat bisa pada jaringan ataupun aplikasi, melakukan klasifikasi data, dan dapat juga berupa pelatihan karena confidentiality bisa juga terancam dikarenakan kelalaian seorang programmer, system administrator dan karyawan lainnya.

  Konsep Confidentiality ini tidak dapat berdiri sendiri, karena juga tergantung dengan konsep Integrity. Tanpa Integrity dijaga dengan baik, maka Confidentiality tidak dapat dipelihara, mari kita bahas dibawah apa itu Integrity.

- Integrity

  Konsep ini bahwa data belum dirusak. Otorisasi diperlukan sebelum data dapat diubah dengan cara apapun; hal ini dilakukan untuk melindungi keaslian data. Mencegah pihak manapun yang tidak berwenang untuk modifikasi, Mencegah pihak yang berwenang dari membuat modifikasi yang tidak ter-otorisasi, misalnya dala suatu system Si A hanya diperbolehkan merubah kolom X, namun ternyata kolom Y jg dapat diubah, baik karena kesalahan system atau tindakan kesengajaan dari si A dan Memelihara konsistensi suatu objek agar data pada objek tersebut benar dan merefleksikan keadaan sebenarnya, dan setiap hubungan dengan objek lainnya menjadi valid, konsisten dan dapat diverifikasi.

  Contohnya : Ancaman serangan pada prinsip Integrity yaitu virus, logic bomb, akses yang tidak terotorisasi, dapat jg berupa error coding dan aplikasi yang menyebabkan data berubah, malicious modification, backdoor dan aktifitas lainnya yang menyebabkan suatu data dan informasi dapat berubah oleh pihak yang tidak berwenang. Lalu berikutnya bagaiman cara mencegah hal ini yaitu dengan membuat akses control yang ketat, menggunakan tools Intrusion Detection System, enkripsi pada objek, menggunakan hash verification untuk memeriksa validitas data, validasi pada system/aplikasi.

- Availability

  Data dapat diperoleh dari bagaimana informasi disimpan, diakses, atau dilindungi. Ini juga berarti bahwa data selalu harus tersedia dari serangan berbahaya yang mungkin dilakukan di atasnya dan menjamin setiap pihak yang berwenang dapat mengakses data, objek dan sumber daya. Pada perusahaan sudah banyak yang menerapkan prinsip ini seperti membuat Disaster Recovery Center, Clustering ataupun Redundancy pada system yang kritikal.

  Contohnya : Biasanya berupa kegagalan perangkat/mesin, error pada software, masalah pada lingkungan seperti banjir, kebakaran, mati listrik, dan juga ancaman hacker seperti DOS Attack juga termasuk yang mengancam prinsip Integrity.

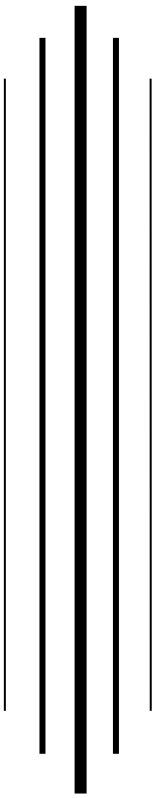
- Accountability

  Pelacakan data, penggunaan komputer, dan sumber daya jaringan. Seringkali itu berarti logging, audit, dan pemantauan data dan sumber daya. Accounting menjadi lebih penting dalam jaringan yang aman. Konsep AAA ini juga harus diterapkan untuk setiap rencana keamanan Anda.

4. Manajemen risiko adalah segala proses kegiatan yang dilakukan semata untuk meminimalkan bahkan mencegah terjadinya risiko perusahaan. Di dalamnya ada kegiatan identifikasi, perencanaan, strategi, tindakan, pengawasan dan evaluasi terhadap hal-hal negatif yang kemungkinan akan menimpa usaha. Untuk memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi maka manajemen harus fokus pada keuangan perusahaan. Deteksinya diarahkan bagaimana sebisa mungkin agar perusahaan tidak kolaps hanya karena dana, modal, laba dan selainnya. Dengan adanya manajemen ini, tentu pihak perusahaan akan memberikan perlindungan terhadap segala aset perusahaan. Tujuannya tidak lain supaya keuangan tetap sehat sehingga bisa dikontribusikan untuk perkembangan usaha ke depan.

5. Administrasi keamanan adalah manajemen dalam sebuat keamanan yang meliputi Kebijakan keamanan teknologi informasi atau kebijakan IT Security merupakan fondasi dari keamanan infrastruktur. Artinya kebijakan ini sangat penting untuk keberlangsungan sistem kedepannya. Kebijakan keamanan diperlukan untuk melindungi dan mengamankan teknologi informasi organisasi. Keuntungan dari kebijakan keamanan: Meningkatkan keamanan data dan jaringan, Mitigasi resiko, Dimonitor dan diaturnya perangkat yang digunakan dan transfer data, Performa jaringan lebih baik, Respon cepat terhadap masalah dan downtime lebih rendah, Mengurangi stress di tingkat manajemen dan Mengurangi biaya.

UAS ADVANCED DATABASE
KELAS MTI 22A



DOSEN PENGASUH

DEDI SYAMSUAR, M.I.T., Ph.D

DISUSUN OLEH:

FADEL MUHAMMAD MADJID

192420052

PROGRAM PASCA SARJANA MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

2020

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!

   Pada proses identifikasi resiko dapat dilakukan pengelompokan resiko berdasarkan sumber daya TI. Salah satu resiko yang dapat diidentifikasi adalah sumber daya manusia meliputi inappropriate access, abuse of position of trust serta disgruntled employees. Dalam pengoperasian IT sebuah organisasi sendiri setiap orang yang memiliki akses terhadap sistem informasi dalam perusahaannya dapat mengakses sesuai dengan wewenang yang dimiliki. Sebagai contoh seorang di bagian IT dalam sebuah bank tentunya memiliki tanggungjawab untuk mengumpulkan dan menganalisis seluruh data keuangan nasabah. Tentunya dalam tanggungjawab pemegang data tersebut terdapat kemungkinan untuk menyelewewengkan wewenang yang telah dimiliki. Sebagai contoh adalah transaksi jual-beli data nasabah bank yang terjadi beberapa waktu yang lalu.

   Contoh kasus:

   Salah satu oknum karyawan bank swasta di bagian IT bernama Hendri menjual data nasabah yang bernama Ilham Bintang (seorang wartawan senior) kepada Desar (seorang pembobol rekening Ilham Bintang). Data nasabah tersebut diperjual belikan oleh Hendri terhadap oknum-oknum yang tentunya bakal disalahgunakan. Salah satu contoh penyalahgunaan data nasabah adalah kasus tersebut. Data nasabah tersebut digunakan untuk membobol kartu kredit Ilham Bintang. Menurut pengakuan Hendri data nasabah diperjualbelikan untuk mendapatkan penghasilan tambahan. Keuntungan dalam transaksi jual beli data nasabah tersebut diperkirakan hingga mencapai Rp 500 juta. Oleh karena perbuatannya Hendri terancam hukuman hingga 20 tahun penjara.

2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?

   SOD merupakan parameter kemanan yang digunakan untuk memperkuat pengamanan system informasi dengan tujuan untuk meminimalisir terjadinya penipuan. Separation of duties (SOD) merupakan suatu langkah untuk memisahkan masing-masing user untuk diberikan wewenang dan tanggungjawab sesuai dengan kebutuhan organisasi. Jika bisnis dijalankan oleh satu role ada kemungkinan terjadinya banyak penipuan dibandingkan dengan situasi yang dimana lebih dari satu role dalam menjalankan bisnis tersebut. Tujuan dari pemisahan ini adalah mengurangi modifikasi data yang tidak sah dalam asset atau informasi dari suatu organisasi serta tindakan preventif terhadap kebocoran data.

   Penerapan SOD dapat diimplementasikan dengan membagi pengontrolan lebih dari satu pengguna untuk menjalankan tugas penting dan sensitif berguna untuk meminimalkan terjadinya peluang untuk melakukan kecurangan sehingga keamanan untuk mengakses system terjamin. Jika role tunggal mendapatkan hak akses untuk membuat, menandatangani serta menyetujui pemesanan pembelian di sebuah department store. Maka memungkinkan peluang kecurangan dalam proses pembelian.

3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!

   Confidentiality (kerahasiaan)

   Confidentiality adalah suatu aspek yang menjamin kerahasian suatu data atau informasi. Kerahasiaan mengandung makna bahwa informasi hanya dapat diakses oleh orang yang berhak mengakses. Usaha-usaha yang dapat dilakukan untuk meningkatkan confidentiality yaitu :

   Teknologi kriptografi

   Kriptografi ini adalah suatu cara untuk mengubah data menjadi bentuk lain (enkripsi) atau istilah awamnya adalah mengubah menjadi kode rahasia atau bentuk sandi-sandi yang sulit untuk dipecahkan (dekripsi). Yang bisa memecahkan kode ini hanya si pemilik data dan si penerima yang valid atau yang benar-benar berhak atas data itu. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

   Otorisasi (authorization) ketat

   Authorization adalah proses pengecekan wewenang user, mana saja hak-hak akses yang diizinkan serta yang tidak diizinkan untuk user. Proses ini dilakukan oleh server dengan cara mengecek hak-hak akses user tersimpan di dalam database. Setelah hak aksesnya diketahui, kemudian server akan menyerahkan hak-hak tersebut kepada user sehingga user telah dapat mengakses resource yang ada didalam jaringan. Tingkat keamanan dari mekanisme otorisasi bergantung kepada tingkat kerahasiaan data yang diinginkan.

   Integrity (integritas)

   Integrity adalah suatu aspek yang menjamin bahwa data atau informasi tidak boleh berubah tanpa seizin pemilik data ataupun pihak yang berwenang. Bentuk serangan terhadap aspek integrity ini seperti : Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

   Availability (ketersediaan)

   Availability adalah suatu aspek yang menjamin ketersediaan sumber data atau informasi jika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh serangan yang dapat mengganggu aspek avalability ini yaitu :

   “denial of service attack” (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.

Mailbomb, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

Accountability

Hal ini bermaksud setiap kegiatan user di dalam jaringan akan direkam (logged). User direkam jejak kegiatannya dilakukan untuk mengenali setiap gerak-gerik yang bakal berpotensi sebagai kejahatan. Oleh karenanya, user akan berpikir dua kali dan tidak akan mencoba-coba untuk melanggar kebijakan keamanan karena identitas dan segala kegiatannya dapat dikenali sehingga mereka dapat dituntut secara hukum. Di dalam sistem yang berbasis accountability murni tidak diterapkan mekanisme access control.

4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!

   Secara umum, risiko didefinisikan sebagai hasil kemungkinan atas kejadian dan dampak dari sebuah kejadian yang dapat terjadi. Dalam teknologi informasi, risiko didefinisikan sebagai hasil dari nilai asset dan kerentanan sistem terhadap risiko dan ancaman yang ditimbulkannya bagi organisasi. Hal ini berarti penerapan dari prinsip-prinisip manajemen risiko terhadap perusahaan yang memanfaatkan teknologi informasi dengan tujuan untuk dapat mengelola risiko-risiko yang berhubungan dengan perusahaan tersebut. Risiko-risiko yang dikelola meliputi kepemilikan, operasional, keterkaitan, dampak, dan penggunaan dari teknologi informasi pada sebuah perusahaan. Tingkat dampak resiko yang dimiliki oleh sebuah proyek pada proses pembuatan proyek serta pengujian juga diperhitungkan. Tentunya dalam pengambilan keputusan tersebut juga didasarkan pada biaya operasional serta keadaan ekonomi perusahaan. Beberapa hal yang patut diperhitungkan meliputi biaya, rangkaian proyek serta kuantitas dari system TI tersebut. Selain itu, perlu adanya strategi mitigasi resiko yang digunakan untuk mengevaluasi, pencegahan serta control terhadap resiko yang bakal dihadapi. 3 strategi yang dapat dikembangkan adalah penghindaran resiko (risk avoidance), pemantauan resiko (risk monitoring) serta perencanaan kontingensi (contingency plan).

5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!

   Anggapan bahwa keamanan sebagai masalah teknis dewasa ini sudah tidak berlaku lagi. Hal tersebut sudah menjadi perhatian utama bagi para pengelola perusahaan/institusi untuk keberlangsungan hidup masing-masing. Para pelanggan sudah mulai khawatir dan menuntut karena kekhawatiran terhadap privasi, perlindungan informasi pribadi. Hal ini disebabkan karena semakin marak terjadinya perilaku criminal di bidang cyber yang dimotivasi oleh keuntungan finansial. Seperti hacking, skimming, defacing, carding, malware dll.

   Tata kelola mengenai keamanan informasi dibutuhkan sebagai dasar pondasi keberlangsungan operasional perusahaan saat ini. Kerangka kerja yang berdasarkan

pada prinsip-prinsip dan persyaratan akuntabilitas digunakan untuk mendorong perilaku yang bijak dalam penggunaan teknologi. Kebijakan serta prosedur dibuat dan dikelola untuk menentukan keamanan informasi bagi para pelanggan maupun perusahaan. Hal ini sangat berpengaruh terhadap para pelanggan yang ingin menikmati produk perusahaan tersebut. Tentunya dibutuhkan pembangunan dan pemeliharaan framework dan struktur manajemen di dalam proses pemberian jaminan keamanan informasi.

Pengusaha, pejabat, direktur dan para pemangku kepentingan memiliki peran dalam mengelola serta bertanggungjawab atas keamanan informasi bagi para pelanggan. Kepercayaan serta reputasi dipertaruhkan jika tata Kelola dan manajemen keamanan tidak dilakukan sebagai mana mestinya. Oleh karenanya dibutuhkan kesadaran akan pentingnya keamanan informasi bagi seluruh orang yang memiliki kepentingan. Keamanan dianggap efektif jika dikelola sebagai berikut:

Keamanan dikelola sebagai masalah perusahaan, secara horizontal, vertikal, dan lintas fungsi di seluruh organisasi. Para pemimpin eksekutif memahami akuntabilitas dan tanggung jawab mereka sehubungan dengan keamanan untuk organisasi, untuk pemangku kepentingan mereka, untuk komunitas yang mereka layani termasuk komunitas Internet, dan untuk perlindungan infrastruktur nasional yang penting dan kepentingan keamanan ekonomi dan nasional.

Keamanan diperlakukan sebagai persyaratan bisnis. Kebijakan keamanan ditetapkan di bagian atas organisasi dengan masukan dari pemangku kepentingan utama. Unit bisnis dan staf tidak diperbolehkan untuk memutuskan secara sepihak seberapa besar keamanan yang mereka inginkan. Pendanaan yang memadai dan berkelanjutan serta alokasi sumber daya keamanan yang memadai diberikan.

Keamanan dianggap sebagai bagian integral dari siklus perencanaan strategis, modal, proyek, dan operasional normal. Keamanan memiliki tujuan yang dapat dicapai dan terukur yang diintegrasikan ke dalam rencana strategis. Oleh karenanya, proyek dapat diimplementasikan dengan kontrol dan metrik yang efektif. Tinjauan dan audit juga dilakukan untuk mengidentifikasi kelemahan dan kekurangan keamanan serta persyaratan untuk kelangsungan operasi. Tujuannya adalah untuk mengukur kemajuan terhadap rencana tindakan dan pencapaian. Lalu menentukan seberapa banyak keamanan yang cukup sama dengan seberapa besar risiko yang dapat ditoleransi organisasi.

Keamanan ditangani sebagai bagian dari setiap inisiasi, akuisisi, atau hubungan proyek baru dan sebagai bagian dari manajemen proyek yang sedang berjalan. Persyaratan keamanan ditangani di seluruh fase siklus hidup pengembangan sistem / perangkat lunak termasuk akuisisi, inisiasi, rekayasa persyaratan, arsitektur dan desain sistem, pengembangan, pengujian, operasi, pemeliharaan, dan penghentian.

Manajer di seluruh organisasi memahami bagaimana keamanan berfungsi sebagai pendukung bisnis. Hal tersebut dapat dijadikan pedoman bahwa keamanan sebagai salah satu tanggung jawab mereka dan memahami bahwa kinerja tim mereka sehubungan dengan keamanan diukur sebagai bagian dari kinerja mereka secara keseluruhan.

Semua personel yang memiliki akses ke aset digital dan jaringan perusahaan memahami tanggung jawab masing-masing terkait dengan perlindungan dan pelestarian keamanan organisasi, termasuk sistem dan perangkat lunak yang digunakan dan dikembangkannya. Kesadaran, motivasi, dan kepatuhan adalah norma budaya yang diterima dan diharapkan. Penghargaan, pengakuan, dan konsekuensi yang berkaitan dengan kepatuhan kebijakan keamanan diterapkan dan diperkuat secara konsisten.

Nama : Isti Ma’atun Nasichah

NIM : 192420051

1. Resiko dalam pengelolaan IT pada dewasa ini semakin menantang. Salah satunya adalah "pembauran antara kehidupan pribadi dan kehidupan sebagai anggota dari suatu perusahaan/organisasi". Anda diminta untuk menerangkan maksud dari pernyataan tersebut. Berikan contoh untuk memperkuat argumentasi anda!

   Jawab :

   Kasus PT Garuda Indonesia dengan dugaan penyelundupan komponen motor dan sepeda di dalam pesawat dengan kerugian negara mencapai Rp 1,5 miliar, yang dinilai pengamat penerbangan sebagai titik terendah kepemimpinan sebuah BUMN. Di samping itu adanya dugaan rekayasa laporan finansial Garuda Indonesia dan penerapan kebijakan Cost-cutting di Garuda selama bertahun-tahun pada awak kabin yang dinilai sangat “zholim” dan sejumlah kebijakan yang merugikan para pekerja di Garuda Indonesia, tindakan sewenang-wenang, dan prostitusi yang berkaitan dengan para direksi dan pejabat Garuda Indonesia. Ari Askhara diberhentikan dari jabatan Dirut Garuda pada tanggal 5 Desember 2019.

   Kasus Ari Ashkara sebagai anggota dari perusahaan/organisasi (sebagai Dirut Garuda Indonesia) itu mau tidak mau akan mempengaruhi kehidupan pribadinya (mempengaruhi reputasi/nama baiknya dalam kehidupan pribadi) dan berdampak mendapatkan sanksi sosial dari masyarakat Hal inilah yang dimaksud pembauran antara kehidupan pribadi dan kehidupan sebagai anggota organisasi/perusahaan.

2. Salah satu prinsip dari keamanan IT adalah "Separation of Duties" atau pemisahan tugas. Silakan ada jelaskan apa dan mengapa prinsip ini perlu diperhatikan dalam manajemen Resiko IT?

   Jawab :

   Idealnya tanggung jawab untuk manajemen IT, pengembangan sistem, operasi, dan pengendalian data seharusnya dipisahkan satu dengan yang lainnya. Pemisahan tugas sangat penting dalam sistem pengendalian internal. Contohnya, karyawan yang merancang sistem

komputer tidak boleh ditugaskan untuk pekerjaan yang menggunakan sistem tersebut, kaerena mereka bisa saja merancang sistem yang menguntungkan mereka secara pribadi dan melakukan kecurangan.

3. Hal yang mendasar dalam keamanan IT adalah CIAA atau Confidential, Integrity, Availability dan Accountability. Jelaskan masing2nya dan berikan contoh untuk memperkuat argumentasi anda!

   Jawab :

   Confidentiality

   Confidentiality merupakan aspek yang menjamin kerahasiaan data atau informasi. Konsep ini mencegah pengungkapan informasi untuk orang yang tidak berhak. Ini di tandai dengan Social Security Numbers (atau identifikasi khusus negara lainnya), informasi SIM, rekening bank dan password, dan sebagainya.
   Sebagai contoh simple jika kita memiliki access point wifi di rumah, lalu tetangga dapat dengan mudah tanpa password untuk menggunakan access point wifi kita, maka dalam hal ini konsep Confidentiality-nya menjadi rendah/hilang.

   Jenis ancaman serangan pada prinsip security ini meliputi mengintip lalu lintas network (biasanya dilakukan di access point wifi public di café atau tempat makan), mencuri password menggunakan social engineering, melakukan port scanning pada server, dan banyak aktivitas lainnya yang berusaha untuk mengambil data atau informasi penting.

   Jika ada ancaman, tentu saja ada langkah pencegahannya, yaitu dengan menerapkan enkripsi pada informasi penting, penerapan akses control yang ketat pada jaringan ataupun aplikasi, melakukan klasifikasi data, dan dapat juga berupa pelatihan karena confidentiality bisa juga terancam dikarenakan kelalaian seorang programmer, system administrator dan karyawan lainnya.

   Integrity

   Integrity merupakan aspek yang menjamin bahwa data tidak boleh berubah tanpa ijin pihak yang berwenang (*authorized*). Agar Integrity dapat dipelihara maka control harus

ditempatkan untuk membatasi akses ke data, objek dan sumber daya. Beberapa contoh terkait ancaman serangan pada prinsip Integrity yaitu virus, logic bomb, akses yang tidak terotorisasi, dapat jg berupa error coding dan aplikasi yang menyebabkan data berubah, malicious modification, backdoor dan aktifitas lainnya yang menyebabkan suatu data dan informasi dapat berubah oleh pihak yang tidak berwenang.

Secara teknis ada banyak cara untuk menjamin aspek integrity ini, seperi misalnya dengan menggunakan *messange authentication code*, *hash function, digital signature*.

Availability

Availability merupakan aspek yang menjamin bahwa data tersedia ketika dibutuhkan. Pada perusahaan sudah banyak yang menerapkan prinsip ini seperti membuat Disaster Recovery Center, Clustering ataupun Redundancy pada system yang kritikal.

Kontrol yang diperlukan dalam menjaga prinsip ini adalah untuk menjamin penanganan cepat ketika terjadi kegagalan system, menyediakan redundancy, memelihara backup, mencegah data hilang atau rusak.

Ancaman serangan pada prinsip ini biasanya berupa kegagalan perangkat/mesin, error pada software, masalah pada lingkungan seperti banjir, kebakaran, mati listrik, dan juga ancaman hacker seperti DOS Attack juga termasuk yang mengancam prinsip Integrity.

Sejumlah pencegahan yang dapat dilakukan terhadap ancaman tersebut seperti dengan menggunakan firewall atau security tools lainnya untuk mencegah DOS, implementasi redundancy untuk system yang kritikal, pemeliharaan backup dan testing backup yang baik dan juga memonitor kinerja lalu lintas jaringan dan system/server.

Accountability

Accountability artinya setiap kegiatan user di dalam jaringan akan direkam (logged) User tidak akan mencoba-coba untuk melanggar kebijakan keamanan karena identitas dan segala kegiatannya dapat dikenali sehingga mereka dapat dituntut secara hukum.

Accountability mencegah illegal behavior. Di dalam sistem yang berbasis accountability murni tidak diterapkan mekanisme access control.

4. Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka. Anda diminta untuk menjelaskan maksud dari pernyataan ini!

   Jawab :

   Manajemen risiko adalah suatu usaha yang dilakukan untuk dapat mengurangi atau menghilangkan risiko yang dihadapi. Penerapkan manajemen risiko dalam konteks organisasi adalah bagaimana suatu organisasi bisa mengelola risiko yang dihadapinya. Manajemen risiko sebagai pelaksanaan fungsi-fungsi manajemen dalam penanggulangan risiko, terutama risiko yang dihadapi oleh organisasi/perusahaan, keluarga dan masyarakat. Manajemen risiko mencakup kegiatan merencanakan, mengorganisir, menyusun, memimpin/mengkoordinir dan mengawasi (termasuk mengevaluasi) program penanggulangan risiko untuk meminimalkan dampak dari kerugian dan ketidakpastian terhadap biaya serta konsekuensinya. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri atas beberapa tahapan kegiatan, ketika diterapkan secara benar memungkinkan terjadinya perbaikan terus menerus dalam proses pengambilan keputusan.

5. Security administration is a management and NOT a purely technical issue. Silakan jelaskan maksud dari pernyataan tersebut!
   Jawab :

   Aspek keamanan dan privasi data (idealnya) menjadi komponen yang harus ada dalam sebuah proses pengembangan produk digital, bukan hanya sekedar dianggap hal teknis saja. Keamanan data dan informasi menjadi tanggung jawab bersama. Pelanggan harus jeli guna membatasi informasi yang diberikan ke penyedia jasa digital dan memahami risiko jika informasi yang diminta terlalu sensitif dan tidak berhubungan dengan jasa.

Keterbatasan pemahaman akan keamanan data ini yang membuat keterlibatan tim *Security* di setiap fase pengembangan sangatlah penting. Tim *Security* dapat meminimalkan terjadinya gangguan terhadap data pelanggan terutama data yang bersifat *privacy* atau rahasia (*personally identifiable information* atau PII). Pengamanan tidak hanya sebatas dari faktor keamanan teknis saat produk digital siap dibuat, namun penerapan pengamanan bahkan harus dilakukan saat produk didesain sesuai dengan standar *best practice*.

Selain itu dalam proses internal, memastikan terdapat aturan yang tegas dalam memberikan hak akses kepada setiap *stakeholder* yang terlibat. *Segregation of duties* atau pemisahan tugas menjadi pendekatan untuk mencegah ancaman dari dalam. Klasifikasi data merupakan pendekatan lain yang bisa dilakukan di dalam *internal business process* untuk menghindari terjadinya data PII terekspos keluar.