Jelaskan perbedaan antara system basis data terpusat, dan sistem basis data terdistribusi

- jawab:

- Sistem basis data terpusat merupakan suatu sistem yang menempatkan data di suatu lokasi saja dan semua lokasi lain mengakses basis data di lokasi tersebut.

- Sistem basis data terdistribusi merupakan sebuah sistem yang berisi kumpulan data logic yang saling berhubungan secara fisik terdistribusi dalam jaringan komputer yang tidak tergantung dari program aplikasi sekarang maupun masa yang akan datang

- Perbedaan antara sistem basis data terpusat dan terdistribusi adalah penggunaan aplikasi yang berhubungan dengan struktur basis data

apa saja dampak dari resiko IT jelaskan beserta contohnya minimal 3!!!

- **Finansial Proyek TI yang mahal gagal menghasilkan dan investasi dihapusbukukan.**
- Contoh: Sydney Water menghabiskan A $ 60 juta untuk informasi pelanggan dan proyek sistem penagihan yang dibatalkan pada akhir tahun 2002 (NSW Auditor-General, 2003).

- **Reputasi Proses bisnis utama yang terlihat oleh publik terhenti karena pemadaman layanan TI.**
- Contoh: Pemadaman ATM Bank of America yang ekstensif pada Januari 2003 disebabkan oleh korupsi server database mereka olehSQL Slammer worm (Infosecurity, 2004).

- **Regulatory Integrity of information mengakibatkan hukuman atas pelanggaran undang-undang**
- Contoh hukum: Tagihan AT&T salah yang mengakibatkan tindakan hukum berhasil oleh Negara Bagian Florida pada tahun 2004.

- **Gagal mematuhi undang-undang.**
- Contoh: 14 tahun setelah undang-undang mengharuskan penjaga pantai untuk mengembangkan sistem identifikasi kapal, tidak sistem seperti itu ada (GAO, 2002).

Sebutkan Jenis Transakasi pada Sistem Basis Data Terdistribusi dan berikan perbedaanya.

jawaban : jenis transaksi pada sistem basis data ini ada 2 yaitu

1. Tranksaksi Lokal

(Transaksi lokal adalah transaksi dari sistem basis data yang dilakukan pada node yang mirip dengan lokasi dimana database berada.)

Update data nasabah Bank yang melakukan penarikan saldo di kantor pusat. Database bank biasanya berada di lokasi yang berdekatan dengan kantor pusat, sehingga bentuk update yang dilakukan di kantor pusat memiliki node yang sama seperti database.

2. Transaksi Global

(Berbeda dengan transaksi lokal, transaksi global menggunakan transaksi dan transmisi data dari berbagai node dengan server atau database yang digunakan)

Seorang nasabah melakukan penarikan saldo di Cabang Bank yang berada di luar pulau. Bank menggunakan server dan database yang sama, namun menggunakan node transmisi data yang berbeda dengan servernya.)

Sebutkan dan jelaskan faktor faktor kegagalan IT ?

- Tidak selarasnya strategi TI dengan strategi perusahaan
- Kurangnya dukungan finansial
- Tidak ada komitmen yang utuh dari manajemen puncak

sebutkan kunci pertimbangan implementasi pada IT Service ?

- 1. menetapkan anggaran dan membelanjakannya dengan tepat,
- 2. menyesuaikan layanan IT dengan konteks resiko yang ada di organisasi,
- 3. mendesogn kapabilitas yang dibutuhkan,
- 4. mengukur dan mengelola kinerja

apakah tujuan dan Manfaat dari Disaster Recovery (DR)?

Tujuan :

- untuk menghilangkan atau mengurangi potensi cedera atau kematian,
- menstabilkan efek bencana,
- melaksanakan rencana DR berdasarkan jenis dan dampak bencana

Manfaat

- Melindungi organisasi dari kegagalan layanan komputer utama

- Meminimalisasi risiko organisasi terhadap penundaan (delay) dalam penyediaan layanan

- Menjamin kehandalan dari sistem yang sedia melalui pengetesan dan simulasi

- Meminimalisasi proses pengambilan keputusan oleh personal/manusia selama bencana.

Sebutkan dan jelaskan secara singkat classes of IT risk!

1. Projects – failing to deliver;

berkaitan dengan kegagalan proyek-proyek TI.

2. IT service continuity – when business operations go off the air;

berkaitan dengan pemadaman layanan TI yang menyebabkan gangguan pada bisnis

3. Information assets – failing to protect and preserve;

berkaitan dengan kerusakan, kehilangan, atau eksploitasi aset informasi

4. Service providers and vendors – breaks in the IT value chain;

penyedia layanan dan vendor memainkan peran penting dalam pengiriman proyek TI dan kegiatan sehari-hari.

5. Applications – flaky systems;

berkaitan dengan kegagalan dalam aplikasi TI.

6. **Infrastructure – shaky foundations; and**

berkaitan dengan kegagalan dalam infrastruktur TI.

7. Strategic and emergent – disabled by IT.

berkaitan dengan kemampuan TI membiarkan eksekusi strategi bisnis.

Sebutkan dan Jelaskan cabang ilmu terapan dari forensik digital ?

- - Computer Forensic, berkaitan dengan forensic digital yang bertujuan untuk mencari serta menganalisis indikasi kejahatan pada komputer untuk memunculkan bukti yang dapat dipergunakan sebagaimana mestinya.
- - Mobile Device Forensic, cabang forensic mengenai akuisisi perangkat seluler untuk memulihkan bukti digital seperti daftar kontak, sms, mms, dll. yang digunakan untukkepentingan investigasi
- - Network Forensic, Cabang ilmu forensic digital untuk menemukan bukti digital seperti sumber serangan keamanan pada suatu jaringan komunikasi/komputer.

Sebutkan dan jelaskan komponen dan proses dalam manajemen risiko. Menurut COSO (Committee of Sponsoring Organizations of the Treadway Commission) !

1. Lingkungan Internal (Internal Environment)

Komponen ini adalah sikap manajemen di semua tingkatan untuk operasi umum dan konsep kontrol pada khususnya.

2. Penentuan Sasaran (Objective Setting)

Perusahaan menetapkan tujuan operasional sebagai dasar untuk mengidentifikasi dan mengelola semua risiko.

3. Identifikasi Peristiwa (Event Identification)

Manajemen mengidentifikasi berbagai peristiwa potensial yang mempengaruhi strategi dan pencapaian tujuan perusahaan. Kejadian tidak pasti ini dapat memiliki dampak positif, tetapi juga dapat memberikan risiko.

4. Penilaian Risiko (Risk Assessment)

Penilaian risiko memungkinkan suatu organisasi untuk menilai suatu peristiwa atau kondisi dan hubungannya dengan pencapaian tujuan organisasi.

5. Tanggapan Risiko (Risk Response)

Manajemen mengevaluasi risiko, kemudian menentukan sikap atau respons terhadap risiko-risiko ini. Respons dari manajemen ini tergantung pada risiko yang dihadapi

6. Aktivitas Pengendalian (Control Activities)

Proses ini adalah persiapan prosedur atau kebijakan yang membantu memastikan bahwa respons terhadap risiko yang dipilih sudah memadai dan dilaksanakan dengan baik.

7. Informasi dan Komunikasi (Information and Communication)

Kegiatan ini berfokus pada pengidentifikasian informasi dan mengkomunikasikannya kepada pihak-pihak terkait melalui media komunikasi yang tepat.

Sebutkan Proses-Proses pada Framework COBIT yang sesuai untuk Manajemen Risiko

- PO1 (Define a Strategic IT Plan) dan PO9 (Assess and Manage Risks)
- AI6 (Manages Change)
- DS5 (Ensure System and Security) DS11 (Manage Data)
- ME1 (Monitor and Evaluate IT Performance)

Sebutkan Hal Apa yang harus kita perhatikan pada setiap tahap proyek organisasi:

- 1. Konsep dan kelayakan
- 2. Persyaratan dan arsitektur
- 3. Pembangunan
- 4. Pengujian, penerimaan dan implementasi
- 5. Pasca implementasi

Apa Fokus Utama dari IT Risk Management ?

- Alasan utama mengapa suatu organisasi perlu untuk menerapkan proses manajemen resiko adalah untuk mendukung misi organisasi dan melindungi aset dari organisasi tersebut.
- Pada IT Risk Management, erat kaitannya dengan bagaimana implementasi security pada suatu organisasi sehingga diperlukan pemahaman tentang proses bisnis organisasi dan kemungkinan resiko yang berdampak pada proses bisnis tersebut.
- Risk Management akan sangat membantu manajemen organisasi untuk menyeimbangkan antara dampak dari risk dan cost yang dibutuhkan untuk meminimalisir resiko tersebut.

Jelaskan 4 langkah manajemen Risiko TI?

1. Identifikasi / penemuan - mendapatkan risiko TI di radar manajemen

2. Penilaian / analisis - memahami risiko TI dalam konteks seluruh portofolio risiko TI dan menilai kemungkinan terjadinya dan dampak potensial pada bisnis

3. Perawatan - menentukan pilihan terbaik dari berbagai tindakan yang mungkin untuk menangani risiko, merencanakan dan menyelesaikan tindakan yang diperlukan

4. Pemantauan dan peninjauan - menindaklanjuti untuk memastikan apa yang direncanakan benar-benar dilakukan dan untuk memahami setiap perubahan lebih lanjut dalam portofolio risiko TI.

Apa yang Dimaksud IT Governance Framework/Kerangka Tata Kelola TI ?

- IT Governance Framework/Kerangka Tata Kelola TI adalah jenis kerangka kerja yang mendefinisikan cara dan metode yang melaluinya suatu organisasi dapat menerapkan, mengelola, dan memantau tata kelola TI dalam suatu organisasi. IT Governance Framework terutama membantu organisasi untuk menyediakan peta jalan dan mengevaluasi kinerja dan efektivitas proses tata kelola TI. Ini memberikan wawasan tentang kinerja departemen TI dan mencapai kepatuhan hukum dan peraturan sehubungan dengan TI.

Sebutkan dan jelaskan Pendekatan portofolio untuk mengumpulkan risiko TI !.....

Kelengkapan : Beberapa bidang risiko TI mungkin diabaikan dalam prioritas yang diberikan kepada yang paling menuntut.

Keterhubungan : Suatu peristiwa tunggal, seperti pengumuman peningkatan atau persyaratan kepatuhan, dapat memiliki banyak dampak di berbagai kelas risiko.

Signifikansi : Dengan menyatukan semua risiko TI dalam sebuah portofolio, konsekuensi berlebihan yang ditimbulkan oleh totalitas risiko akan terlihat jelas.

Apa saja ketentuan dari Aset Informasi?

kerahasiaan

Aset informasi hanya dapat diakses hanya oleh mereka yang berhak mengaksesnya

Integritas

Aset informasi harus benar - mutakhir, akurat dan dapat diverifikasi -

ketersediaan

Aset informasi harus dapat diakses saat dibutuhkan

kepatuhan

Manajemen aset informasi harus memenuhi hukum eksternal, tata kelola dan persyaratan peraturan

Jelaskan apa fungsi security awareness dan berikan contoh security awareness ?

- Security awareness atau kesadaran akan keamanan adalah pengetahuan dan sikap dari setiap orang dalam organisasi terhadap kepedulian keamanan aset informasi dan data dari organisasi tersebut. Menjadi sadar terhadap keamanan sistem berarti memahami bahwa ada potensi bagi ancaman yang sengaja atau tanpa sengaja mencuri, melakukan pengrusakan, atau penyalahgunaan data yang disimpan dalam sistem komputer perusahaan dan seluruh organisasi. Oleh karena itu, maka akan lebih bijaksana untuk mendukung aset lembaga (informasi, fisik, dan pribadi) dengan mencoba untuk menghentikan hal itu terjadi.

Contoh :

1. Data dan informasi dalam media yang sudah tidak digunakan lagi misalnya dalam harddisk komputer yang rusak hendaknya dihancurkan, agar tidak dapat dibaca oleh orang yang tidak berhak.
2. Kebijakan terhadap password dan penggunaan otentikasi dua faktor.
3. Masing-masing pengguna dibiasakan untuk selalu logout dari aplikasi dan tidak meninggalkan dalam keadaan masih login.
4. Menyimpan username dan kata sandi untuk login ke berbagai aplikasi dengan baik dantidak memberikan informasi tersebut kepada orang lain.

sebutkan dan jelaskan gambaran umum drp (Disaster Recovery Plan)

-Pengkajian dan Pembaharuan berkala

Kegiatan pengkajian dan pembaharuan IT-DRP harus dilakukan secara terstruktur dan terkontrol. Setiap perubahan yang dilakukan dalam IT-DRP harus diuji secara penuh sesuai dengan kondisi perusahaan. Sehingga seluruh perubahan yang dilakukan dalam IT-DRP ini harus dikontrol dan dengan persetujuan dari Direktur IT perusahaan.

-Penyimpanan IT-DRP

Salinan dari IT-DRP, CD, dan hard copy akan disimpan di dalam lokasi aman yang ditentukan oleh perusahaan. Setiap anggota dari manajer senior harus memiliki salinan dari IT-DRP yang harus disimpan di dalam tempat tinggal setiap anggota. Selain itu setiap anggota Disaster Recovery Team (DRT) harus memiliki salinan dari IT-DRP tersebut.

-Tugas dan Tanggung Jawab DRT (Disaster Recovery Team)

Disaster Recovery Team (DRT) merupakan personil inti dari DRP yang bekerja dibawah pengawasan CIO atau Manajer IT Senior perusahaan. DRT bertugas untuk menerapkan DRP ketika terjadi bencana dalam perusahaan, dan memastikan bahwa DRP diterapkan secara menyeluruh.

-Respon Terhadap Keadaan Darurat

Merupakan prosedur-prosedur yang harus dilakukan ketika terjadi suatu bencana mendadak. Hal ini ditujukan agar ketika terjadi bencana tersebut, tim dapat menyediakan baik pertolongan pertama maupun prosedur evakuasi.

-Apendiks

Sesuai dengan standar NIST SP 800-34, maka dalam dokumen ini akan dilampirkan formulir yang berisi tentang gambaran teknis setiap peralatan dan operasionalnya.

apa penyebab inkonsistensi data secara tidak sengaja

penyebabnya inkonsistensi data secara tidak sengaja ada 3

- proses pemasukan data (data entry) yang tidak benar
- proses pembaharuan data (update) yang tidak benar
- pengendalian sistem yang tidak baik/kontrol

Kerugian akibat peristiwa Risiko IT yang terjadi pada perusahaan, dapat ditangani IT dengan mengurangi atau mengendalikan risiko. Sejauh mana IT dapat memberikan kontribusi penanganan peristiwa risiko tersebut.

- Pencurian eksternal dan penipuan yang dilakukan melalui saluran elektronik dapat dikurangi melalui peningkatan otentikasi TI dan metode control akses
- Kegagalan penangkapan, eksekusi dan pemeliharaan transaksi dapat dikurangi melalui peningkatan antarmuka pengguna, validasi dat, dan pemeriksaan integritas di titik masuk dan alur kerja berbasis aturan untuk mengelola pemrosesan
- Pengungkapan informasi kepada klien dapat dibuat lebih konsisten melalui pengiriman informasi on-line

Sebagai pimpinan atau penanggung jawab tertentu dalam perusahaan,apa saja fungsi–fungsi yang dapat audara lakukan dalam melakukan pengelolaan terhadap resiko yang berhubungansecara langsung maupun tidak langsung dengan perusahaan?

Jika saya sebagai pimpinan yang bertanggung jawab atas pekerjaan yang saya lakukan untuk pengelolaan resiko adalah hal pertama yang dilakukan mencari tahu resiko yang terjadi bersumber darimana. Misalkan contoh resikonya adalah hilangnya sejumlah asset yang sudah tercatat dibuku jurnal tidak sama dengan jumlah nyata. Maka akan dilakukan pengecekan terperinci mengenai seluruh catatan – catatan keluar masuknya asset – asset tersebut. Jika telah ditemukan kesalahan dalam pencatatan asset tersebut maka resiko telah ditemukan, yang berarti pengelolaan resiko sudah lebih ringan. Tetapi, tidak hanya begitu saja, kesalahan yang menyebabkan timbulnya resiko itu akan dievaluasi agar tidak terjadi berulang kali dan tidak dalam jangka waktu yang lama yang dapat merugikan perusahaan. Jadi, bila terjadi resiko yang sama perusahaan sudah mempunyai tekhnik yang tepat untuk mengatasi resiko tersebut. Selanjutnya, setelah kita mengelola resiko tersebut, kita belajar dari resiko yang kita dapat beserta cara mengelolanya. Jadi kita bisa lebih baik dalam mengelola resiko yang telah dipelajari dari pengelolaan sebelumnya.

Sebutkan dan jelaskan contoh Manfaat dari melakukan Manajemen Resiko Bisnis?

1. dapat di jadikan sebagai bahan evaluasi dan pengambilan keputusan.

evaluasi adalah suatu proses pengukuran efektivitas strategi yang anda pakai dalam menjalankan bisnis anda pada masa yang sudah lewat. dari hasil evaluasi yang anda lakukan kemudian anda dapat menjadikannya sebagai tolak ukur dalam pengambilan keputusan untuk langkah selanjutnya.

2. dapat meningkatkan produktifitas serta menambah keuntungan

Melalui manajemen resiko, kita tentunya lebih berhati-hati dalam menjalankan bisnis agar terhindar dari resiko yang sama. hal ini sangat membantu kita dalam meningkatkan produktivitas serta menambah keuntungan, jika di bandingkan sebelum kita menggunakan manajemen resiko.

3. dapat memudahkan dalam estimasi biaya

dengan adanya analisa dan manajemen resiko sangat mempermudah anda dalam menghitung estimasi biaya yang digunakan untuk keperluan bisnis anda. misalnya keperluan produksi dll.

Bagaimana IT bisnis akan mendukung strategi bisnis Anda?

- Transformasi digital pasti akan membutuhkan dukungan IT yang kuat mengingat ada banyak software atau perangkat teknologi baru yang digunakan.Dengan asumsi bahwa Anda sudah memiliki strategi bisnis yang jelas, sebaiknya Anda kembali mengevaluasi strategi IT bisnis selama 3-5 tahun ke depan. Dengan begini, Anda bisa memastikan agar strategi IT sejalan dengan transformasi digital yang dilakukan di perusahaan. Anda juga dapat menghitung biaya yang harus dikeluarkan untuk melakukan transformasi ini.

IT risk management meliputi tiga proses sebutkan:

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

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

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.