Ujian Akhir Semester

Mata Kuliah : IT Risk Management & Disaster Recovery
Semester : Ganjil – 2020/2021
Kelas : MTI

Petunjuk:

- Anda diminta untuk menjawab soal-soal. Setiap jawaban anda akan dinilai berdasarkan pengetahuan yang tercermin dari jawaban anda
- Setiap soal bernilai sama yaitu 20 %.
- Jawaban akan dicek dengan menggunakan aplikasi TURNITIN untuk memeriksa kesamaan jawaban mahasiswa satu dengan laiinya.

Soal :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

Selamat bekerja
Semoga kesuksesan selalu menyertai anda

NAMA : M. Iqbal Rivana
NO MHS : 192420057
MK : IT Risk Management
Dosen : Dedy Syamsuar, M.I.T, Ph.D

Soal :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

Jawaban :

Merupakan proses yang digunakan untuk mengurangi dan mengelola risiko yang mungkin terjadi dalam infrastruktur IT yang ada atau sistem yang diterapkan dalam organisasi. Manajemen risiko memegang peranan penting sebagai tindakan perlindungan asset sistem dan teknologi informasi. Manajemen risiko meliputi tiga proses besar yaitu:

1. Risk Assessment : adalah proses awal dalam manajemen risiko untuk memetakan tingkat ancaman yang potensial dan risiko yang ada dalam SDLC IT.
2. Risk Mitigation : adalah langkah yang melibatkan usaha untuk memprioritaskan, mengevaluasi dan menjalankan control atau pengendalian yang dapat mengurangi risiko yang tepat yang diinisiasi dari proses risk assessment.
3. Evaluation dan Assessment : evaluasi dan penilaian ulang terhadap risiko yang ada dan yang telah terjadi.

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

Jawaban:

Integrity yaitu taraf kepercayaan terhadap sebuah informasi. Dalam konsep ini tercakup data integrity dan source 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. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

Jawaban :

Karena dengan dilakukannya penilaian risiko terhadap suatu insiden IT maka kita bisa mendapatkan informasi dan dapat melakukan analisis berdasarkan bukti untuk membuat keputusan berdasarkan informasi tentang bagaimana mengontrol risiko tertentu dan bagaimana memilih metode kontrol di antara beberapa pilihan yang ada.

Dengan menggunakan penilaian risiko, sebuah organisasi dapat membuat keputusan yang lebih baik mengenai risiko dan mencapai tujuan bisnisnya. Menghilangkan ketidakpastian dengan menilai risiko memungkinkan sebuah organisasi mengelola operasinya dengan tingkat kepercayaan diri tertentu. Pemahaman ini mengantarkan pada sebuah keputusan apakah risiko yang telah teridentifikasi dapat diterima atau tidak, dan tindakan pengendalian apa yang paling tepat. Pada akhirnya, “output” dari penilaian risiko merupakan “input” terhadap proses pengambilan keputusan.

Contoh:

1. Kasus pembobolan uang nasabah rekening Commonwealth Bank atas nama ilham bintang yaitu salah satu produser acara televisi ternama. Berikut kronologi kasus nya.

Pelaku beraksi ketika Ilham berada di Australia pada 30 Desember 2019 hingga 14 Januari 2020. Tanggal 4 Januari 2019, ia hendak menuju Melbourne menggunakan pesawat. Waktu setempat menunjukkan pukul 5 pagi, ia tersadar kartu SIM Indosat yang ia gunakan berstatus 'SOS', dia tidak yakin apakah karena gangguan sinyal atau masa berlaku paket roaming telah habis.

Karena harus naik pesawat, ia acuhkan sementara status itu. Pukul 9 pagi, Ilham tiba di Melbourne, memutuskan membeli kartu lain dari provider Optus. Dengan harapan tidak ada kendala ketika ingin bertransaksi menggunakan internet banking di rekening Commonwealth Bank miliknya, ia menjajal Optus.

Tanggal 5 Januari, dia tidak bisa memasukkan akun dan kata kuncinya di aplikasi internet banking, Ia menduga ada yang membajak kartu SIM-nya, "Pelaku mengambil dolar Australia (AUD), lalu dipindahkan ke rupiah," ucap Ilham. Dia mencoba menelusuri, meminta jejak transfer pelaku. Ditemukan 94 transaksi ke akun belanja online, pelaku pun menyebar duit rampokan itu ke beberapa rekening.

94 transaksi terduga pelaku terdiri dari: 28 Domestic Transfer, 62 Bill Payment, 2 Internal Account Transfer dan 2 kolom kosong. Mereka beraksi 4 Januari (40 transaksi), 5 Januari (50 transaksi), dan 6 Januari (4 transaksi). Ada 82 transfer berstatus completed, 12 lainnya rejected. Pelaku menggunakan 92 transaksi mobile dan 2 transaksi internet, sedangkan user type ialah retail. Ilham mengaku hanya rekening Commonwealth Bank miliknya yang dibobol dan ludes saldonya, sedangkan saldonya di rekening bank lainnya aman. Pelaku mentransfer duit Ilham Bintang ke rekening BNI, Mandiri BRI, BCA dan LinkAja. Akibat kejadian ini, Ilham merasa dirugikan ratusan juta rupiah.

(Pembobol Rekening Ilham Bintang Jual Data Nasabah Hingga Rp500 Juta - Tirto.ID)

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

Jawaban :

Disaster Recovery Plan **(DRP)** adalah suatu pernyataan yang menyeluruh mengenai tindakan konsisten yang harus diambil sebelum, selama, dan setelah suatu peristiwa yang mengganggu dan menyebabkan suatu kerugian penting sumber daya sistem informasi.*Disaster recovery plan*adalah prosedur untuk merespons suatu keadaan darurat, menyediakan*backup*operasi selama gangguan terjadi, dan mengelola pemulihan dan menyelamatkan proses sesudahnya.

Sasaran pokok*Disaster RecoveryPlan* adalah untuk menyediakan kemampuan dalam menerapkan proses kritis di lokasi lain dan mengembalikannya ke lokasi dan kondisi semula dalam suatu batasan waktu yang memperkecil kerugian kepada organisasi, dengan pelaksanaan prosedur *recovery* yang cepat.

Secara umum tujuan DRP yang utama adalah untuk menyediakan suatu cara yang terorganisir untuk membuat keputusan jika suatu peristiwa yang mengganggu terjadi. Tujuan*Disaster RecoveryPlan* adalah untuk mengurangi kebingungan organisasi dan meningkatkan kemampuan organisasi untuk berhubungan dengan krisis tersebut.

Ketika suatu peristiwa yang mengganggu terjadi, organisasi tidak akan mempunyai kemampuan untuk menciptakan dan melaksanakan suatu rencana pemulihan dengan segera. Oleh karena itu, jumlah perencanaan dan pengujian yang telah dilakukan sebelumnya akan menentukan kemampuan organisasi tersebut dalam mengangani suatu bencana.

DRP mempunyai banyak sasaran, dan masing-masing sasaran tersebut penting. Sasaran-sasaran tersebut meliputi:

- Melindungi suatu organisasi dari kegagalan penyediaan jasa komputer.
- Memperkecil risiko keterlambatan suatu organisasi dalam menyediakan jasa
- Menjamin keandalan sistem melalui pengujian dan simulasi
- Memperkecil pengambilan keputusan oleh personil selama suatu bencana

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

Jawaban :

Penilaian teknologi adalah pengamatan dan evaluasi terhadap semua bentuk teknologi baru. Hal ini didasarkan pada anggapan bahwa semua penemuan teknologi baru tidak hanya berguna bagi kalangan ilmuwan yang menemukan dan membuat teknologi itu saja, tetapi juga bermanfaat untuk masyarakat luas. Bentuk evaluasi yang lain berkaitan dengan pengamatan mengenai apakah pemanfaatan produk teknologi itu tidak mempunyai implikasi etis dan sosial dalam masyarakat, seperti menyalahi kerahasiaan pribadi (*privacy right)* misalnya. Penilaian teknologi juga melihat segi positif dan negatif dari pemakaian teknologi itu. Kadang kala, penilaian teknologi harus melihatnya dalam perpektif global, dan wawasan ke depan. Suatu penilaian teknologi akan cenderung menerima bentuk inovasi baru,

karena pertimbangan aplikasinya pada masa mendatang, dan tidak hanya sekadar menolak segala bentuk pembaharuan yang tidak menguntungkan bagi sekelompok masyarakat tertentu. Oleh karena itu hasil dari penilaian teknologi ini harus dipublikasikan agar diketahui oleh masyarakat umum, dan dikomunikasikan dengan kalangan politikus pengambil keputusan. Badan internasional yang berkaitan dengan hal ini disebut ICENT *(International Convention for The Evaluation of New Technologies)*.

Saat ini perusahaan dan organisasi banyak menghabiskan dana untuk investasi dibidang IT. Manfaat IT dalam peningkatan layanan dan proses kerja sebuah organisasi sangat terasa. Dengan investasi yang cukup besar organisasi perlu memastikan kehandalan dan keamanan dari sistem IT yang akan digunakan. Sistem IT juga harus mampu memenui kebutuhan proses kerja, mampu mengurangi resiko data di sabotasi, kehilangan data, gangguan layanan dan manajemen yang buruk dari sistem IT.

Audit TI atau yang pernah disebut sebagai *audit electronic data processing*, *computer information system*, dan IS, pada awalnya merupakan pelebaran dari *audit konvensional*. Dulu, kebutuhan atas fungsi audit TI hanya berasal dari beberapa departemen. Kemudian auditor sadar bahwa komputer telah mempengaruhi kinerja mereka terkait fungsi utama. Perusahaan dan manajemen pemrosesan informasi pun sadar bahwa komputer adalah jalan keluar terkait permasalahan sumber daya untuk semakin bersaing dalam lingkungan bisnis bahkan antar departemen. Oleh karenanya, muncullah urgensi untuk melakukan kontrol dan audit atas proses yang berjalan. Saat itulah para profesional menyadari tentang kebutuhan audit TI. Audit TI menjadi bagian integral dalam fungsi audit umum, sebab hal itu akan menentukan kualitas dari informasi yang diproses oleh sistem komputer.

Pada mulanya, auditor dengan kemampuan audit TI dilihat sekadar sebagai staf sumber daya teknologi biasa, bahkan sering dilihat hanya sebagai asisten teknikal. Padahal dewasa ini, audit IT merupakan pekerjaan yang tindakan, tujuan, serta kualitasnya telah diatur dalam standar global; ada aturan etiknya; dan tuntutan profesional. Tentu saja hal ini memerlukan pengetahuan khusus dan kemampuan praktis, yang sebelumnya juga didahului oleh persiapan secara intensif.

UAS IT RISK MANAGEMENT & DISASTER RECOVERY

OLEH :

NANDA S.PRAWIRA 192420056

Semester : Ganjil – 2020/2021
Kelas : MTI

Petunjuk:

- Anda diminta untuk menjawab soal-soal. Setiap jawaban anda akan dinilai berdasarkan pengetahuan yang tercermin dari jawaban anda
- Setiap soal bernilai sama yaitu 20 %.
- Jawaban akan dicek dengan menggunakan aplikasi TURNITIN untuk memeriksa kesamaan jawaban mahasiswa satu dengan laiinya.

Soal :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?
2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi
3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)
4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?
5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

Jawab.

1. Mengapa it risk management penting di terapkan di dalam oganisasi karena untuk melindungi organisasi dari resiko yang menghambat dan juga menghalangi tujuan dari organisasi tersebut serta resiko Teknis dan non Teknis mungkin melanda suatu organisasi maka dari itu risk manajemen sangat penting bagi organisasi untuk melindungi organisasi, meningkatkan kinerja organisasi, serta melindungi data data yang terdapat di hardware organisasi.

2. Dalam dunia digital, informasi menjadi aset yang sangat berharga dimana pertukaran informasi dan data menjadi sangat cepat dan mudah. Dengan kemudahan yang didapat karena kemajuan teknologi, tentu memunculkan pula ancaman terhadap keamanan informasi. Maka dari itu integritas dalam perusahaan sangat di butuhkan karena dengan semakin mudahnya pertukanan informasi dan dengan integritas yang baik maka informasi yang di kirim tidak ada perubahan dan sampai tujuan dengan aman. Namun jika Terdapat pihak- pihak yang memiliki integritas buruk dan tidak bertanggung jawab melakukan tindakan illegal demi mendapatkan informasi yang diinginkan yang membuat kerugian di dalam organisasi dan hanya menguntungkan dirinya sendiri.

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Menurut (Anisah Herdiyanti, 2018) OGC Self-Assessment Tools ini dikembangkan berdasarkan best practice manajemen layanan teknologi ITILyang terbagi menjadi lima area dimana dalam setiap area dijabarkan dalam beberapa proses. Penelitian ini berfokus pada area Service Operation yaitu pada fungsi service desk. Service Operation merupakan fase kritis dari siklus hidup manajemen layanan. Proses yang direncanakan dan dilaksanakan dengan baik akan sia-sia jika operasional seharihari dari proses-proses tersebut tidak dilakukan, dikontrol dan dikelola dengan benar. Juga perbaikan layanan tidak akan mungkin dilakukan jika kegiatan sehari-hari untuk memantau kinerja, menilai metrik dan mengumpulkan data tidak dilakukan secara sistematis selama layanan beroperasi [4]. Terdapat sejumlah proses kunci Service Operation yang harus dihubungkan bersama-sama untuk memberikan struktur dukungan IT yang efektif secara keseluruhan, antara lain [1] Incident Management, Problem Management, Request Fulfilment, Event Management, dan Access Management. Self-assessment didasarkan pada kuesioner terstruktur khusus untuk setiap proses dengan setiap pertanyaan yang membutuhkan

jawaban YES atau NO. Setiap perntanyaan memiliki nilai berdasarkan bobotnya. Tools ini menyediakan pendekatan yang fleksibel dan mudah digunakan dan dibangun pada Microsoft Excel dan karena itu dapat diselesaikan dengan mudah [5]. Hasil penilaian akan segera diberikan dalam bentuk grafik dan memberikan perbandingan skor yang didapatkan versus target yang ditetapkan "praktik baik" untuk setiap elemen dari kerangka manajemen proses [6]. OGC Self-Assessment menggunakan kerangka manajemen proses yang terdiri dari sembilan level proses yang digambarkan dengan pertanyaan. Contoh level OGC Self-Assessment beserta deskripsi dan poin utama pertanyaan level ditunjukan pada Tabel 1.

Tabel 1. Contoh Penjelasan Sistem Penilaian OGC *Self-Assessment*

Capability Level	Deskripsi	Poin Utama Pertanyaan Level
Level 1 Prerequisites	Organisasi telah memenuhi tingkat minimal item prasyarat untuk mendukung kegiatan proses	Ketersediaan proses dalam organisasi dan ketersediaan posisi fungsional maupun pihak yang bertanggung jawab pada proses tersebut
Level 1.5 Management Intent	Adanya dukungan manajemen dalam mendorong pelaksanaan proses dalam organisasi	Ketersediaan kebijakan dan prosedur yang terkait dengan proses, dukungan manajemen pada staf dalam menjalankan kegiatan proses
Level 2 Process Capability	Setiap kegiatan proses telah dilakukan organisasi untuk mendukung pelaksanaan proses	Identifikasi apakah aktifitas minimal yang harus dilakukan dalam proses telah atau sedang dilakukan oleh organisasi
Level 2.5 Internal Integration	Aktifitas-aktifitas proses dalam organisasi telah terintegrasi	Memastikan apakah aktifitas-aktifitas terintegrasi dan cukup untuk memenuhi tujuan proses

4. Menurut (Akmal Hidayat, 2012) encana penanggulangan bencana (Disaster Recovery Plan) adalah salah rencana darurat dibidang teknologi info rmasi yang ditujukan untuk pemulihkan layanan IT setelah terjadinya suatu gangguan besar/bencana dan membutuhkan relokasi system. DRP didefinisikan secara berbeda beda oleh oleh masing masing organisasi. Perbedaan tersebut disebabkan perbedaan persepsi, fungsi dan dan kepentingan setiap organisasi. Namun DRP tidak boleh didefinisikan keluar dari tujuan dan batasan DRP.

   Dalam melakukan perencanaan DRP, dilakukan identifikasi misi utama organisasi (mission-critical), penting dan tidak pentingnya proses, sistem dan layanan dalam jaringan untuk memastikan perlindungannya terhadap resiko bencana yang ada. Elemen kunci dari perencanaan DRP adalah :

   a .Membentuk tim perencana; Tim yang dibentuk terdiri dari pengambilkeputusan dari setiap unit usaha atau area operasional, bertanggung jawab atas semua aktivitas DRP, perencanaan dan melaporkan perkembangan yang terjadi setiap bulannya pada manajemen senior.

b.Melakukan penilaian resiko dan audit; Untuk membuat rencana DRPtim tersebut harus memahami proses bisnis, teknologi, jaringan dan layanan. Analisa resiko dan analisa dampak usaha setidaknya dilakukan terhadap 10 besar potensi bencana. Analisa dilakukan dengan mempertimbangkan skenario terburuk yaitu dari kehilangan atau kerusakan total fasilitas. Analisa juga dilakukan dengan mempertimbangkan aspek geografis, rancangan sistem IT saat ini dan layanan yang tersedia. Setiap analisa harus menggambarkan dampak finansial dari pernggantian perangkat, alokasi sumberdaya tambahan dan kontrak pemasangan layanan tambahan.

5. Peninjauan kembali terhadap standard yang telah ditetapkan bertujuan untuk menetapkan kemunginan terjadinya dan dampak suatu suatu kejadian yang menghambat pencapaian tujuan atau sasaran organisasi supaya dapat dilakukan penanganan risiko secara tepat. Tujuan tersebut dapat dicapai melalui identifikasi risiko dan analisis risiko. Manfaat penilaian risiko antara lain, membantu pencapaian tujuan organisasi, menjaga kesinambungan pelayanan kepada para stakeholder, melakukan pelayanan secara efektif dan efisiensi menjadi dasar penyusunan rencana strategis, dan menghindari terjadinya pemborosan.

IT RISK MANAGEMENT & DISASTER RECOVERY

(UJIAN AKHIR SEMESTER)

NAMA : RAHMI
NIM : 192420046

Soal :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

Jawab :

1. IT Risk Management adalah 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.
   Hambatan umum terhadap data dan sistem teknologi informasi meliputi:
   a) Kerusakan perangkat keras dan perangkat lunak
   b) *Malware*
   c) Virus computer
   d) *Spam, scams, and phishing*
   e) *Human error*
   Selain hambatan umum, dalam IT Risk Management juga mengelola hambatan criminal terhadap teknologi informasi suatu perusahaan, antara lain:

a) *Hackers*, yaitu orang-orang yang secara tidak sah menerobos ke dalam sistem computer
b) *Fraud*, yaitu penggunaan computer untuk memanipulasi data untuk kepentingan yang melanggar hokum
c) *Denial-of-service*, yaitu serangan *online* yang membuat pengguna tidak dapat mengakses situs tertentu
d) *Staff dishonesty*, yaitu pencurian data atau informasi penting oleh karyawan internal.

2. Integritas, Semua sistem dan subsistem yang dibangun harus mampu memberikan gambaran yang lengkap dan akurat dari sistem fisik yang diwakilinya. Aspek ini menekankan bahwa informasi tidak boleh tanpa seijin pemilik informasi. Adanya virus, Trojan horse, atai pemakai lain yang mengubah informasi tanpa ijin merupakan contoh msalah yang harus dihadapi. Sebuah email dapat saja "ditangkap" (intercept) di tengah jalan, diubah isinya (altered, tampered, modified), kemudia diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan enkripsi dan digital signature, misalnya, dapat mengatasi masalah ini. Salah satu contoh kasus Trojan hosre adalah distribusi paket program TCP Wrapper (yaitu program popuker yang dapat digunakan untuk mengatur dan membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak bertanggung jawab. Jika anda memasang program yang berisi Trojan horse tersebut, amak ketika anda merakit (compile) program tersebut, dia akan mengirimkan email kepada oarng tertentu yag kemudian memperbolehkan dia masuk ke system anda. Informasi ini berasal dari CERT Advisory, "CA-99-01 Trojan-TCP-Wrappers" yang didistribusikan 21 Januari 1999. Contoh serangan lain aalah yang disebut "man in the middle attack" dimana seseorang menempatkan diri di tengan pembir=caraan dan menyamar sebagai orang lain.

3. Membangun control internal yang kuat dalam teknologi informasi yang dapat membantu organisasi untuk meningkatkan pemahaman tentang TI di kalangan eksekutif. Semua itu didapat untuk meningkatkan kompetensi.

4. *Disaster Recovery* dirancang khusus dengan tujuan untuk melakukan *recovery* atau pemulihan pada suatu sistem apabila terjadi bencana alam.

5. Karena manajemen risiko merupakan suatu proses mengidentifikasi, mengukur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Manejemen risiko bertujuan untuk mengelola risiko sehingga dapat memperoleh hasil yang optimal. Agar dapat berjalan dengan baik, manajemen risiko diletakkan dalam suatu kerangka manajemen risiko. Prinsip dari Manajemen Risiko: Prinsip dasar untuk penerapan manajemen risiko pada proses bisnis adalah Pertama,

memahami apa saja sasaran (objektif) proses bisnis tersebut. Kedua, mengidentifikasi apa saja yang dapat menghambat tercapainya sasaran. bisnis proses tersebut. Ketiga, pengendalian apakah yang harus dilakukan agar risiko-risiko tersebut dapat ditiadakan atau dikurangi.

Ujian Akhir Semester

Nama : Rani Okta Felani

Kelas : MTI 22

Mata Kuliah : IT Risk Management & Disaster Recovery
Semester : Ganjil – 2020/2021
Kelas : MTI

Petunjuk:

- Anda diminta untuk menjawab soal-soal. Setiap jawaban anda akan dinilai berdasarkan pengetahuan yang tercermin dari jawaban anda
- Setiap soal bernilai sama yaitu 20 %.
- Jawaban akan dicek dengan menggunakan aplikasi TURNITIN untuk memeriksa kesamaan jawaban mahasiswa satu dengan laiinya.

Soal :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

Selamat bekerja
Semoga kesuksesan selalu menyertai anda

Jawaban :

1. IT Risk Managemen penting di terapkan dalam suatu organisasi karena peran risk management (manajemen resiko) dalam mengelola resiko- resiko yang di hadapi BANK. Sama halnya dengan perusahaan lainnya, perbankan perlu mengelola manajemen resiko dengan baik, apalagi jika termasuk klasifikasi perusahaan besar dan mempunyai beberapa anak perusahaan yang tersebar di berbagai titik. Perlunya suatu proses identifikasi, analisis penilaian dan monitoring suatu resiko yang sangat cepat perubahannya pada perbankan dan kemudian perlu segera dilakukan pengukuran atas mitigasi resiko untuk kepentingan *stakeholder's* dan dalam menyeimbangkan *Risk and reward.*

Ada beberapa alasan mengapa manajemen risiko diperlukan dalam perbankan:

1. Merupakan salah satu aspek dalam *good corporate govermance*
2. Membantu *Top Management Bank* dalam proses pengambilan keputusan bisnis
3. Tersedianya ukuran penilaian secara kualitatif dan kuantitatif
4. Mendorong bank beroperasi secara lebih efisien (*more developed risk measurement*)
5. Mengantisipasi penerapan internal model (*standard* s.d *advanced*)
6. Sebagai sarana *early warning system* bagi *risk management unit* dan *risk management committee*
7. Meningkatkan *shareholder's value* (*ultimate objective*)

Hambatan umum terhadap data dan sistem teknologi informasi meliputi :

a. Kerusakan perangkat keras dan perangkat lunak
b. Malware
c. Virus Computer
d. Spam, Scams, and Phising
e. Human error

2. Penerapan prinsip integritas dalam keamanan teknologi informasi

Integrasi : adanya saling keterkaitan antar sub sistem sehingga data dari satu sistem secara rutin dapat melintas, menuju atau diambil oleh satu atau lebih sistem yang lain.

Sistem integrasi (integrated system) merupakan sebuah rangkaian proses untuk menghubungkan beberapa sistem komputerisasi dan software aplikasi, baik secara fisik maupun secara fungsional. Sistem terintegrasi akan menggabungkan komponen sub-sub

sistem ke dalam satu sistem dan menjamin fungsi-fungsi dari sub sistem tersebut sebagai satu kesatuan sistem.

Pengintegrasian sistem informasi merupakan salah satu konsep kunci dari sistem Informasi Manajemen. Berbagi sistem dapat saling berhubungan satu dengan yang lain dengan berbagai cara yang sesuai dengan keperluannya. Aliran informasi diantara sistem sangat bermanfaat bila data dalam file suatu sistem diperlukan juga oleh sistem yang lainnya, atau output suatu sistem menjadi input bagi sistem lainnya. Secara manual juga dapat dicapai suatu integrasi tertentu, misalnya data dari satu bagian dibawa kebagian lain, dan oleh petugas administrasi data tersebut digabung dengan data dari sistem yang lain. Jadi kalau secara manual maka derajat integrasinya menjadi tinggi.

Konsep Integrasi sistem adalah yaitu suatu konsep sistem yang dapat saling berhubungan satu dengan yang lain dengan berbagai cara yang sesuai dengan keperluan. Hal ini sangat bermanfaat bila suatu data dalam file suatu sistem diperlukan juga oleh sistem yang lainnya atau output sustu sistem menjadi Input sistem lainnya.

Keuntungan dari integrasi sistem ini adalah membaiknya suatu arus informasi dalam sebuah organisasi. Suatu pelaporan biasanya memang memerlukan waktu, namun demikian akan semakin banyak informasi yang relevan dalam kegiatan manajerial yang dapat diperoleh bila diperlukan. Keuntungan ini merupakan alasan yang kuat untuk mengutamakan (mengunggulkan) sistem informsi terintegrasi karena tujuan utama dari sistem informasi adalah memberikan informasi yang benar pada saat yang tepat. Keuntungan lain dari pengintegrasian sistem adalah sifatnya yang mendorong manajer untuk membagikan (mengkomunikasikan) informasi yang dihasilkan oleh departemen (bagian) nya agar secara rutin mengalir ke system lain yang memerlukannya.

Suatu pelaporan biasanya memang memerlukan waktu, namun demikian akan semakin banyak informasi yang relevan dalam kegiatan manajerial yang dapat diperoleh bila diperlukan. Keuntungan ini merupakan alasan yang kuat untuk mengutamakan (mengunggulkan) sistem informsi terintegrasi karena tujuan utama dari sistem informasi adalah memberikan informasi yang benar pada saat yang tepat.

Integrasi informasi dari sebuah sistem diperlukan karena :

1. Adanya kebutuhan konstituen untuk bekerja sama antar Organisasi Perangkat Daerah (OPD) dalam suatu pemerintahan.
2. Terjadinya pengolahan data antar sistem informasi tiap OPD yang saling terkait, sehingga untuk melengkapi suatu informasi dibutuhkan proses pertukaran data dengan sistem informasi yang lain.

3. Dapat memungkinkan penyediaan realtime pengaksesan data.
4. Mengubah data untuk analisis dan pertukaran data, mengatur penempatan data untuk kinerja.

3. Membangun control internal yang kuat dalam teknologi informasi dapat membantu organisasi untuk meningkatkan pemahaman tentang TI di kalangan eksekutif, membuat keputusan bisnis yang lebih baik dalam kualitas yang lebih tinggi dan informasi lebih tepat waktu, menyelaraskan berbagai inisiatif proyek dengan kebutuhan bisnis, mencegah hilangnya sumber daya dan kemungkinan pelanggaran sistem (fox dan zobbeveld,2013). Semua itu digunakan untuk mengoptimalkan teknologi informasi dalam meningkatkan kompetensi.

4. *Disaster Recovery* dirancang khusus dengan tujuan untuk melakukan *Recovery* atau pemulihan pada suatu sistem apabila terjadi sesuatu seperti bencana alam, kegagalan operasional sistem (seperti update yang gagal) atau kesalahan manusia pada Pusat Data utama sebuah perusahaan.

   Disaster Recovery plan atau rencana pemulihan bencana jarang terjadi karena dijadikan prioritas oleh pelaku bisnis dan memerlukan biaya yang cukup mahal serta penerapan yang sulit, terlebih Karena bencana adalah hal yang tidak dapat di duga oleh manusia. Hal ini membuat para pelaku bisnis berpikir bahwa *Disaster Recovery plan* tidak di prioritaskan . padahal pihak lain mengganggap bahwa nilai data perusahaan yang tersimpan di data center merupakan nyawa dari bisnis perusahaan tersebut. Oleh karena itu tingkat urgensi pembuatan *Disaster Recovery* sebagai keberlangsungan bisnis. Rencana pemulihan bencana atau DRP adalah pendekatan yang terdokumentasi dan terstruktur dengan instruksi untuk mengatasi insiden yang tidak direncanakan. Drp melibatkan analisis proses bisnis dan kebutuhan keberlanjutan. *Disaster Recovery* bertujuan untuk meminimalkan resiko dan optimalisasi kesinambungan entitas dalam menghadapi resiko bencana.

5. Manajemen Resiko merupakan suatu proses mengidentifikasi, mengukur resiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Manajemen resiko bertujuan untuk mengelola resiko sehingga dapat memperoleh hasil yang optimal. Prinsip dasar untuk penerapan manajemen resiko pada proses

bisnis adalah , memahami apa saja sasaran objektif proses bisnis tersebut. Serta mengidentifikasi apa saja yang dapat menghambat tercapainya sasaran. Bisnis.

IT RISK MANAGEMENT & DISASTER RECOVERY (MTIK232)

Nama : Sigit Pamungkas

NIM : 192420047

1. **Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?**

IT Risk Management sangat penting dalam organisasi karena merupakan proses yang digunakan untuk mengurangi dan mengelola risiko yang mungkin terjadi dalam infrastruktur IT yang ada atau sistem yang diterapkan dalam organisasi. Manajemen risiko memegang peranan penting sebagai tindakan perlindungan asset sistem dan teknologi informasi.

2. **Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi.**

Keamanan komputer atau dalam Bahasa Inggris computer security atau dikenal juga dengan sebutan cybersecurity atau IT security adalah keamanan informasi yang diaplikasikan kepada komputer dan jaringannya. Computer security atau keamanan komputer bertujuan membantu user agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi. Informasinya sendiri memiliki arti non fisik.

Contohnya dalam suatu system perbankan, tentunya data tersebut harus reel dengan yang terjadi sesungguhnya. Karena kalau tidak reel dengan data sesungguhnya maka system tersebut telah gagal. Dan apabila terjadi perubahan mendesak maka diperlukan izin dari pemegang system tersebut atau atasan yang bertugas.

3. **Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)**

Pada perusahaan yang memiliki sumberdaya yang besar berupa bahan baku, sumberdaya manusia, maupun barang jadi sudah saatnya menggunakan sistem komputerisasi yang terintegrasi agar lebih effisien dan effektif dalam memproses data yang dibutuhkan. Sistem Informasi dalam suatu perusahaan bertujuan untuk mencapai tiga tujuan utama: kerahasiaan, ketersediaaan, dan integrasi.

a. Kerahasiaan. Untuk melindungi data dan informasi dari penggunaan yang tidak semestinya oleh orang-orang yang tidak memiliki otoritas. Sistem informasi eksekutif,

sumber daya manusia, dan sistem pengolahan transaksi, adalah sistem-sistem yang terutama harus mendapat perhatian dalam keamanan informasi.

b. Ketersediaan. Supaya data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya.
c. Integritas. Seluruh sistem informasi harus memberikan atau menyediakan gambaran yang akurat mengenai sistem fisik yang mereka wakili.

Dalam mengelola aset informasi sebuah organisasi, para Manajer Teknologi Informasi (TI) atau Chief Information Officer (CIO) membutuhkan kebijakan keamanan informasi, yang memberikan pedoman mengenai prosedur, aturan dan hal-hal lain yang berhubungan dengan pengelolaan informasi.

Oleh karena itu assessment dalam insiden IT perlu dilakukan dalam manajemen risiko karena untuk melakukan tindakan IT sesuai perkembangan zaman harus dilakukan untuk mempermudah pekerjaan di dalam suatu organisasi. Namun selain kemudahan yang dilihat, kita juga harus melihat risiko yang akan dialami apabila ingin menggunakan IT seperti biaya yang diperlukan, proses pembukuan/mengalihkan data yang sudah ada didalam pembukuan ke dalam IT.

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

Disaster recovery adalah berfungsi untuk melindungi serta menyelamatkan data ketika terjadi bencana, baik bencana alam maupun kerusakan yang disebabkan oleh kelalaian manusia. Sistem tersebut dapat diterapkan dalam berbagai bentuk dengan pendekatan yang berbeda-beda. Berikut adalah beberapa jenis sistem pemulihan bencana yang sering digunakan oleh perusahaan atau organisasi untuk melindungi data-data pentingnya.

a. Disaster Recovery Virtual
   Seperti namanya, recovery jenis ini mengandalkan metode virtualisasi dalam proses pemulihan data. Pusat data virtual ditempatkan untuk menggantikan server fisik sebagai perangkat utama. Tak jarang, metode ini juga didukung oleh sejumlah portal virtualisasi yang menghadirkan layanan backup dan restore.
   Ketika terjadi bencana atau kerusakan, sistem pemulihan virtual akan segera melakukan tindakan penyelamatan data tanpa menunggu server fisik menyelesaikan beban kerjanya. Oleh karena itu, jenis recovery ini dianggap lebih menguntungkan dari segi efisiensi waktu.
b. Disaster Recovery Jaringan
   Tipe kedua disaster recovery berpusat pada pemulihan jaringan. Metode ini berkembang dari asumsi bahwa jaringan suatu perusahaan merupakan aspek penting yang harus turut diselamatkan saat bencana melanda. Prosedur pemulihan jaringan umumnya melibatkan koneksi dengan anggota tim IT, penggantian perangkat jaringan, serta sejumlah usaha terkait lain untuk memulihkan konektivitas yang sempat terputus.
c. Disaster Recovery dalam Pusat Data
   Pemulihan yang berpusat pada data center atau pusat data perusahaan ditempatkan dalam sebuah sistem khusus yang menggunakan fasilitas komputerisasi. Untuk bisa melakukan proses manajemen bencana, pusat data tersebut harus dikembangkan terlebih dahulu.

Prosedur pengembangannya meliputi pengamanan lokasi, pemantapan perangkat dan pegawai, serta pengaturan HVAC ruangan (heating, ventilation, dan air conditioning).
Disaster recovery pusat data dianggap sebagai solusi paling aman dan efektif bagi sebagian besar perusahaan. Namun, waktu pengembangan yang cukup panjang serta banyaknya unsur penting yang harus dilibatkan membuat jenis manajemen bencana ini sering dirasa kurang praktis.

d. Disaster Recovery Berbasis Cloud
Jenis terakhir yang juga menjadi jenis paling populer saat ini adalah manajemen bencana berbasis cloud. Proses intinya berpusat pada cloud storage, yakni portal penyimpanan dan pemulihan data yang diatur oleh penyedia layanan pihak ketiga.
Dengan menggunakan cloud-based disaster recovery, perusahaan akan memiliki pusat data aman di dalam cloud tanpa perlu mengembangkan fasilitas sendiri atau mempekerjakan tenaga ahli. Seluruh prosedur pengamanan data pun dijalankan secara lebih praktis.

Salah satu contoh dari jenis disaster recovery ini adalah Azure Site Recovery. Dengan menggunakan pusat data berbasis cloud services, layanan tersebut akan membantu Anda memulihkan data saat terjadi bencana. Prosedur perlindungan dan pemulihan data yang dijalankan juga didukung oleh infrastruktur yang lengkap serta layanan yang terintegrasi luas.

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

Dalam IT yang telah menerapkan Manajemen Risiko sangat penting untuk melakukan peninjauan kembali dalam standard yang telah dilakukan karena apabila system IT tersebut sangat berisiko fatal maka perlu adanya persetujuan dari atasan atau organisasi untuk melihat apakah risiko yang telah ditemukan tersebut dapat teratasi dengan baik dan apakah ada kendala apabila system tersebut nantinya telah digunakan.

Ujian Akhir Semester

NAMA : SUWANI

NIM : 192420049

Mata Kuliah : IT Risk Management & Disaster Recovery
Semester : Ganjil – 2020/2021
Kelas : MTI

Petunjuk:

- Anda diminta untuk menjawab soal-soal. Setiap jawaban anda akan dinilai berdasarkan pengetahuan yang tercermin dari jawaban anda
- Setiap soal bernilai sama yaitu 20 %.
- Jawaban akan dicek dengan menggunakan aplikasi TURNITIN untuk memeriksa kesamaan jawaban mahasiswa satu dengan laiinya.

Soal :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi.

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

Selamat bekerja
Semoga kesuksesan selalu menyertai anda

Jawaban !

1. IT Risk Management penting diterapkan dalam suatu organisasi karena Pada zaman digital sekarang ini, banyak organisasi menggunakan *Information Technology* (IT) sebagai bagian dari sistem yang memproses informasi untuk menunjang misi dan keberlangsungan organisasi mereka. Sehingga IT sekarang ini memegang peranan yang sangat penting bagi kelangsungan suatu organisasi. Sebagaimana kita tahu komponen IT terdiri dari *software* dan *hardware*, yang mana terkadang ditemukan *vulnerability* di dalamnya. Belum lagi adanya ancaman (*threat*) intrusi baik dari luar maupun dalam yang dapat mengancam proses bisnis suatu organisasi.

2. contoh, penerapan prinsip integritas dalam keamanan teknologi informasi yaitu
   User mengembangkan dan mengevaluasi kebuthan fungsional, atau system informasi operasi dalam organisai, System Engineers dan arsitek yang merancang, mengimplementasikan, atau memodifikasi system informasi, yang bertujuan untuk mencapai keamanan informasi tahapan pengamanan yang dapat memenuhi keamanan system informasi.

3. Membangun kontrol internal yang kuat dalam Teknologi Informasi (TI) dapat membantu organisasi untuk meningkatkan pemahaman tentang TI di kalangan eksekutif, membuat keputusan bisnis yang lebih baik dalam kualitas yang lebih tinggi dan informasi lebih tepat waktu, menyelaraskan berbagai inisiatif proyek dengan kebutuhan bisnis, mencegah hilangnya sumber daya dan kemungkinan pelanggaran sistem. Pengukuran layanan IT dengan menggunakan maturity level pada insiden, dengan menggunakan metode deskriptif dan metode kuantitaif (kusioner). Dilakukan sebagai langkah untuk melihat tingkatan kematangan dari divisi Technical support. Dengan diketahuinya tingkatan/level tersebut akan mudah menentukan proses selanjutnya guna meningkatkan layanan TI tersebut. Pengukuran difokuskan pada manajeman insiden pada divisi Technical Support. Pembuatan dokumen tatalaksana dikembangkan sebagai tujuan utama untuk membantu divisi helpdesk dalam melakukan pendokumentasian dan mendukung layanan IT yang terdiri dari 10 aktifitas,yang dibangun untuk menjadi kesimpulan keseluruhan proses program. Matriks dalam dokumen tatalaksanan yang dibuat berisikan masing-masing aktifitas dalam program berikut dengan tujuan, indicator

kinerja, formulir dan dokumen yang diperlukan untuk pelaksanaan aktifitas,yang digunakan untuk menilai terhadap setiap prosedur dalam pelaksanaan manajemen insiden di UPT STMIK AMIKOM Yogyakarta.

Kutipan : *Jurnal Manajemen Insiden dalam Pengelolaan Infrastruktur Teknologi Informasi (Studi Kasus UPT Laboratorium STMIK Amikom Yogyakarta) Tri Susanto Program Studi Teknik Informatika Program Pascasarjana, STMIK AMIKOM Yogyakarta, Jurnal Telematika Vol. 5 No.2 Agustus 2012*

4. IT Disaster Recovery Plan merupakan stretegi untuk membuat perencanaan perlindungan terhadap aset IT, karena saat ini IT sudah menjadi aset penting dalam perusahaan, aset-aset yang perlu di lindungi ini meliputi, Data, Infrastruktur IT, Aplikasi. Sebuah Bisnis harus dapat mengembangkan rencana pemulihan bencana terhadap aset TI. Yang dimulai dengan menyusun inventarisasi perangkat keras (misalnya server, desktop, laptop, dll), aplikasi perangkat lunak dan data. Rencana tersebut harus mencakup strategi untuk memastikan bahwa semua mendukung informasi penting. Mengidentifikasi aplikasi perangkat lunak dan data penting serta hardware yang dibutuhkan untuk menjalankannya. Yang dapat digunakan untuk membantu mereplikasi konfigurasi ke hardware baru. memastikan bahwa salinan program perangkat lunak yang tersedia untuk memungkinkan instalasi ulang pada peralatan pengganti. Dengan memprioritaskan hardware dan software pemulihan. Mendokumentasikan perencenaan pemulihan IT dari bencana sebagai bagian dari rencana kesinambungan bisnis. Menguji rencana berkala untuk memastikan bahwa strategi pemulihan ini dapat bekerja.

5. Karena untuk melihat nilai Tingkat Kematangan Penerapan manajemen risiko dalam kreteria berhasil itu ditunjukkan dengan adanya identifikasi dan analisis risiko sesuai tingkat kepentingannya. Risiko dimitigasi, dilacak, dan dikendalikan secara efektif. Permasalahan dicegah sebelum terjadi dan pegawai secara sadar fokus pada apa yang akan mempengaruhi pencapaian tujuan.

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

UJIAN AKHIR SEMESTER

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

Penyelesaian :

Seperti yang kita ketahui perkembangan teknologi di zaman digital sekarang ini sangat diperlukan dalam suatu organisasi karena kebanyakan organisasi menggunakan IT sebagai penunjang misi dan keberlangsungan organisasi dalam suatu sistem organisasi agar dapat memproses informasi.

Dalam sebuah informasi pada organisasi tentunya dibutuhkan sebuah keamanan yang dapat mengamankan suatu informasi pada organisasi, maka dari itu sangat diperlukan / diterapkan sebuah IT Risk Management yang berfungsi untuk memproses identifikasi kerentanan ancaman terhadap sebuah informasi yang digunakan dan dilakukan oleh suatu organisasi untuk mencapai tujuan, mengurangsi resiko dan menyeimbangkan pengeluaran dalam mencapai keberlangsungan organisasi dalam bagian IT.

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi.

Penyelesaian :

Salah satu contoh penerapan prinsip integritas dalam keamanan teknologi informasi yaitu salah satunya pada perangkat desktop malware disebarkan melalui perangkat lunak atau kode program. Saat menggunakan perangkat desktop dan ingin menginstal perangkat lunak Anda perlu berhati-hati dalam mengeksekusi kode programnya. Bisa jadi aplikasi yang Anda unduh merupakan aplikasi yang sudah disusupi malware di dalamnya. Ketika dieksekusi maka malware otomatis akan menyebar di dalam sistem. Tidak jarang di dalam kode program terdapat backdoor yang digunakan untuk memberikan hak akses kepada pembuat malware supaya dapat mengakses sistem dari jarak jauh.

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silahkan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

Penyelesaian :

Risk assessment atau yang lebih akrab disebut dengan penilaian risiko, merupakan sebuah metode yang banyak digunakan pada berbagai organisasi atau sebuah pekerjaan. Banyak yang mengartikan bahwa, risk assessment adalah suatu metode yang secara sistematis digunakan untuk menentukan dan meminimalisir risiko yang akan terjadi pada sebuah organisasi.

Sistem metode ini merupakan sebuah kunci, yang mana dapat Anda gunakan dalam perencanaan pemulihan sebuah bencana. Pada dasarnya, dalam melakukan sebuah penilaian risiko terdapat beberapa tahap. Mulai dari proses menganalisis dan menafsirkan kemungkinan-kemungkinan terburuk atau risiko yang akan terjadi.

Risiko sering dianggap sebagai bentuk atau akibat dan dampak negatif dari adanya suatu kegiatan. Umumnya identik dengan sesuatu yang menimbulkan kerugian. Dengan berbagai bidang usaha yang berbeda tentunya kemungkinan risiko yang dihadapi juga berbeda-beda. Sebagai contoh, pada proyek konstruksi tentu memiliki karakteristik dan kondisi yang berbeda.

Sumber-sumber penyebab risiko tentunya juga berbeda. Umumnya terbagi menjadi 4 hal, antara lain :

1. Risiko Operasional, merupakan sebuah risiko yang disebabkan oleh para manusianya, alam atau bahkan teknologi.
2. Risiko Eksternal, adalah risiko yang umumnya atau biasanya hadir dan berasal dari lingkungan luar perusahaan atau proyek.
3. Risiko Internal, sebuah risiko yang tentunya berasal dari dalam diri perusahaan itu sendiri.
4. Risiko Keuangan, yakni sebuah risiko yang telah disebabkan oleh faktor keuangan. Umumnya seperti adanya perubahan harga, mata uang dan bahkan tingkatan suku bunga.

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

Penyelesaian :

Disaster Recovery adalah fasilitas atau prosedur untuk memperbaiki dan/atau mengembalikan kerusakan/dampak suatu bencana ke kondisi semula. Disaster recovery plan ini juga meliputi kemampuan untuk prosedur organisasi dan “back up” pemrosesan, penyimpanan, dan basis data.

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

Penyelesaian :

Pentingnya melakukan peninjauan kembali terhadap standar yan telah ditetapkan sangat diperlukan sebagai proses yang bertujuan untuk membantu organisasi memahami, menilai dan mengambil tindakan pada semua risiko dengan maksud untuk meningkatkan kemungkinan keberhasilan dan mengurangi kemungkinan kegagalan.

UJIAN AKHIR SEMESTER

IT RISK MANAGEMENT& DISASTER RECOVERY

Oleh : YAYAN CANDRA SUBIDIN

NIM : 192420054

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA PALEMBANG

TAHUN 2020

Ujian Akhir Semester

Mata Kuliah : IT Risk Management& Disaster Recovery

Semester : Ganjil – 2020/2021

Kelas : MTI

Petunjuk:

- Anda diminta untuk menjawab soal-soal. Setiap jawaban anda akan dinilai berdasarkan pengetahuan yang tercermin dari jawaban anda
- Setiap soal bernilai sama yaitu 20 %.
- Jawaban akan dicek dengan menggunakan aplikasi TURNITIN untuk memeriksa kesamaan jawaban mahasiswa satu dengan laiinya.

Soal :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

   Jawab :

   IT Risk Management penting diterapkan dalam suatu organisasi karena :

   a) Menjadi panduan untuk mengidentifikasi risiko yang dihadapi dan mengukur serta menentukan besarnya risiko tersebut sehingga dapat mencari jalan dari penyelesaian resiko secara efektif.
   b) Menyusun strategi untuk memperkecil ataupun menanggulangi risiko yang terjadi.
   c) Mengkoordinir pelaksanaan penanggulangan risiko serta mengevaluasi program penanggulangan risiko yang telah di buat
   d) Menghemat waktu, biaya dan tenaga dengan alat untuk mengatasi risiko bisnis

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

   Jawab :

   Integrity Keamanan informasi menjamin kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya. Pengertian lain dari integrity adalah memastikan bahwa informasi tersebut masih utuh, akurat, dan belum dimodifikasi oleh pihak yang tidak berhak.

   Contohnya penerapannya antara lain:

   Communication security yang merupakan keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada didalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.

   Network security yang merupakan keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

   Jawab :

   Guna mengetahui seberapa besar ancaman risiko yang didapatkan oleh perusahaan tersebut, sehingga dapat menentukan tindak lanjut yang benar berdasarkan tolak ukur yang telah ada. Dengan adanya prioritas yang jelas maka akan dapat didefinisikan kontrol - kontrol mana saja yang perlu diterapkan

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

   Jawab :

   Disaster (bencana) didefinisikan sebagai kejadian yang waktu terjadinya tidak dapat diprediksi dan bersifat sangat merusak. Dalam bisnis, Disaster Recovery dikenal dengan Disaster Recovery Plan yang merupakan prosedur yang dijalankan ketika BCP berlangsung. DRP berisi langkah-langkah untuk penyelamatan dan pemulihan yang biasanya focus pada fasilitas IT dan sistem informasi. DRP merupakan pengaturan yang comprehensive yang berisikan tindakan-tindakan yang harus dilakukan sebelum, selama dan setelah adanya bencana yang mengakibatkan hilangnya sumber daya informasi. DRP juga berisi prosedur dalam merespon kejadian darurat, operasi backup cadangan disaat system berhenti dan pengelolaan proses perbaikan serta penyelamatan agar meminimalisir kerugian yang dialami.

   Adapun tujuan utama DRP agar sumber daya dalam menjalankan proses vital pada lokasi cadangan dapat tersediakan dan mengembalikan fungsi lokasi utama menjadi normal pada batas waktu tertentu, dengan cara menjalankan prosedur pemulihan secara cepat untuk meminimalisir kerugian.

   Proses-proses yang terkandung dalam DRP dalam mengurangi resiko terhadap penggunaan IT bagi organisasi sebagai berikut:
   - ✓ Proses Disaster Recovery Planning
   - ✓ Pengujian Disaster Recovery Plan
   - ✓ Prosedur Pemulihan Bencana

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

   Jawab :

   Guna memeriksa kembali apakah standart yang telah diterapkan sesuai dengan resiko yang akan dihadapi kedepannya sehingga dapat menghasilkan strategi penanganan risiko yang lebih baik

UJIAN AKHIR SEMESTER

IT RISK MANAGEMENT& DISASTER RECOVERY

Oleh : AL ADRI NOFA GUSANDI

NIM : 192420053

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA PALEMBANG

TAHUN 2020

Ujian Akhir Semester

Mata Kuliah : IT Risk Management& Disaster Recovery

Semester : Ganjil – 2020/2021

Kelas : MTI

Petunjuk:

- Anda diminta untuk menjawab soal-soal. Setiap jawaban anda akan dinilai berdasarkan pengetahuan yang tercermin dari jawaban anda
- Setiap soal bernilai sama yaitu 20 %.
- Jawaban akan dicek dengan menggunakan aplikasi TURNITIN untuk memeriksa kesamaan jawaban mahasiswa satu dengan laiinya.

Soal :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

   Jawab :

   IT Risk Management penting diterapkan dalam suatu organisasi karena :

   a) Menjadi panduan untuk mengidentifikasi risiko yang dihadapi dan mengukur serta menentukan besarnya risiko tersebut sehingga dapat mencari jalan dari penyelesaian resiko secara efektif.
   b) Menyusun strategi untuk memperkecil ataupun menanggulangi risiko yang terjadi.
   c) Mengkoordinir pelaksanaan penanggulangan risiko serta mengevaluasi program penanggulangan risiko yang telah di buat
   d) Menghemat waktu, biaya dan tenaga dengan alat untuk mengatasi risiko bisnis

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

   Jawab :

   Integrity Keamanan informasi menjamin kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya. Pengertian lain dari integrity adalah memastikan bahwa informasi tersebut masih utuh, akurat, dan belum dimodifikasi oleh pihak yang tidak berhak.

   Contohnya penerapannya antara lain:

   Communication security yang merupakan keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada didalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.

Network security yang merupakan keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

Jawab :

Guna mengetahui seberapa besar ancaman risiko yang didapatkan oleh perusahaan tersebut, sehingga dapat menentukan tindak lanjut yang benar berdasarkan tolak ukur yang telah ada. Dengan adanya prioritas yang jelas maka akan dapat didefinisikan kontrol - kontrol mana saja yang perlu diterapkan

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

Jawab :

Disaster (bencana) didefinisikan sebagai kejadian yang waktu terjadinya tidak dapat diprediksi dan bersifat sangat merusak. Dalam bisnis, Disaster Recovery dikenal dengan Disaster Recovery Plan yang merupakan prosedur yang dijalankan ketika BCP berlangsung. DRP berisi langkah-langkah untuk penyelamatan dan pemulihan yang biasanya focus pada fasilitas IT dan sistem informasi. DRP merupakan pengaturan yang comprehensive yang berisikan tindakan-tindakan yang harus dilakukan sebelum, selama dan setelah adanya bencana yang mengakibatkan hilangnya sumber daya informasi. DRP juga berisi prosedur dalam merespon kejadian darurat, operasi backup cadangan disaat system berhenti dan pengelolaan proses perbaikan serta penyelamatan agar meminimalisir kerugian yang dialami.

Adapun tujuan utama DRP agar sumber daya dalam menjalankan proses vital pada lokasi cadangan dapat tersediakan dan mengembalikan fungsi lokasi utama menjadi normal pada batas waktu tertentu, dengan cara menjalankan prosedur pemulihan secara cepat untuk meminimalisir kerugian.

Proses-proses yang terkandung dalam DRP dalam mengurangi resiko terhadap penggunaan IT bagi organisasi sebagai berikut:

- ✓ Proses Disaster Recovery Planning
- ✓ Pengujian Disaster Recovery Plan
- ✓ Prosedur Pemulihan Bencana

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

   Jawab :

   Guna memeriksa kembali apakah standart yang telah diterapkan sesuai dengan resiko yang akan dihadapi kedepannya sehingga dapat menghasilkan strategi penanganan risiko yang lebih baik

Ujian Akhir Semester

Nama : Arpa Pauziah
NIM : 192420055
Mata Kuliah : IT Risk Management & Disaster Recovery
Semester : Ganjil – 2020/2021
Kelas : MTI

Petunjuk:

- Anda diminta untuk menjawab soal-soal. Setiap jawaban anda akan dinilai berdasarkan pengetahuan yang tercermin dari jawaban anda
- Setiap soal bernilai sama yaitu 20 %.
- Jawaban akan dicek dengan menggunakan aplikasi TURNITIN untuk memeriksa kesamaan jawaban mahasiswa satu dengan laiinya.

Soal :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

Jawab :
Pentingnya IT Risk Management dalam menerapkan prinsip-prinsip manajemen resiko bagi organisasi perusahaan dan memanfaatkan teknologi informasi untuk tujuan agar dapat mengelola resiko yang berhubungan dengan organisasi tersebut. Adapun resiko yang di kelola meliputi operasional, keterkaitan, penggunaan teknologi informasi, kepemilikan dan dampak.

Resiko umum terhadap data dan sistem teknologi informasi meliputi :
1. Malware
2. Spam, scams dan phishing
3. Human error
4. Dan berbagai macam kerusakan perangkat keras dan perangkat lunak lainnya.

Selain resiko umum yang biasa terjadi ada pula ancaman kriminal terhadap teknologi informasi pada suatu organisasi yaitu Hackers, fraud, denial of service, staff dishonesty.

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

Jawab:
Salah satu contoh prinsip integritas dalam suatu keamanan teknologi infirmasi yaitu dengan menerapkan digital signature atau tanda tangan digital sehingga dapat menjamin agar data tidak dapat berubah tanpa izin dari pihak yang berwenang.

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

Jawab :
Assessment adalah salah satu tahapan manajemen bisnis. Penilaian Risiko (Risk Assessment) dalam manajemen bisnis digunakan untuk menentukan prioritas dari risiko-risiko yang teridentifikasi.

Ada tiga tahapan dalam penilaian risiko yaitu :

1. Identifikasi Risiko (Risk Identification), Merupakan proses menemukan, mengenali dan menggambarkan risiko

2. Memperkirakan Risiko (Risk Estimation)/ Analisa Resiko (Risk Analysis)

3. Risk Evaluation tujuan dari evaluasi risiko adalah untuk membantu dalam membuat keputusan , berdasarkan hasil analisis risiko, resiko mana yang memerlukan perbaikan dan prioritas untuk dilakukan lebih awal.

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

Jawaban :
Disaster Recovery atau Pemulihan Bencana melibatkan serangkaian kebijakan, alat, dan prosedur untuk memungkinkan pemulihan atau kelanjutan infrastruktur dan sistem teknologi penting setelah bencana alam atau yang disebabkan oleh manusia. Disaster Recovery berfokus pada TI atau sistem teknologi yang mendukung dalam mengurangi resiko terhadap penggunaan IT bagi organisasi, yang melibatkan menjaga semua aspek penting dari fungsi sebuah organisasi meskipun terjadi peristiwa mengganggu yang signifikan. Oleh karena itu, Disaster Recovery dapat dianggap sebagai bagian dari kelangsungan suatu organisasi. Disaster Recovery mengasumsikan bahwa situs utama tidak dapat dipulihkan (setidaknya untuk beberapa waktu) dan merupakan proses pemulihan data dan layanan ke situs sekunder yang selamat, yang berlawanan dengan proses pemulihan kembali ke tempat asalnya.

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

Jawab:
pentingnya melakukan peninjauan kembali terhadap standard yang telah ditetapkan untuk melihat apa adanya dalam pelaksanaannya. Hal ini merupakan upaya untuk memastikan bahwa sistem manajemen risiko berjalan sesuai dengan rencana yang telah disetujui dan sejalan dengan program ruang lingkup.

Berbagai organisasi di Indonesia telah mulai menerapkan kerangka kerja manajemen risiko berbasis ISO 31000: 2009 mengenai *Manajemen* Risiko- *Prinsip dan Pedoman* . Pelaksanaan manajemen risiko dalam suatu organisasi juga harus didukung dengan peningkatan risiko oleh para pelaku program, karena risiko risiko pada perubahan lingkungan baik internal maupun eksternal. Dengan demikian, risiko dapat dihindari.

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

1. Memberikan hasil program yang lebih baik karena pengambilan keputusan yang tepat.
2. Mengakui adanya ketidak pastian / risiko dengan 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.

NAMA : ELPINA SARI

NIM : 192420050

UAS : IT RISK MANAGEMENT

SOAL :

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

JAWABAN :

1. Karena dengan menggunakan *Information Technology* (IT) sebagai bagian dari sistem yang memproses informasi untuk menunjang misi dan keberlangsungan organisasi mereka. Sehingga IT sekarang ini memegang peranan yang sangat penting bagi kelangsungan suatu organisasi. Sebagaimana kita tahu komponen IT terdiri dari *software* dan *hardware*, yang mana terkadang ditemukan *vulnerability* di dalamnya. Belum lagi adanya ancaman (*threat*) intrusi baik dari luar maupun dalam yang dapat mengancam proses bisnis suatu organisasi. Adanya kemungkinan *threat* dan *vulnerability* tersebut otomatis menimbulkan *risk* (resiko) yang mungkin dapat menghabiskan *cost* (biaya) yang tidak terduga. Pentingnya IT Risk Management, untuk mengetahui bagaimana pentingnya dan proses manajemen resiko pada suatu organisasi untuk meminimalisir resiko dan menjamin resiko tetap pada level yang dapat diterima. Pentingnya menggunakan IT Risk Management agar mengetahui proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang digunakan oleh sebuah organisasi dan dilakukan oleh manajer IT untuk mencapai tujuan bisnis,mengurangi resiko, dan menyeimbangkan pengeluaran dalam mencapai keuntungan dan melindungi IT.

2. Prinsip Integrity menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, Trojan horse atau pemakai lain yang mengubah informasi tanpa izin. contoh sebuah e-mail dapat saja “ditangkap” (intercept) di tengah jalan, diubah isinya (altered, tampered, modified), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan enkripsi dan digital signature, misalnya, dapat mengatasi masalah ini.Salah satu contoh kasus trojan horse adalah distribusi paket program TCP Wrapper (yaitu program popular yang dapat digunakan untuk mengatur dan membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak bertanggung jawab. Jika anda memasang program yang berisi trojan horse tersebut, maka ketika anda merakit (compile) program tersebut, dia akan

mengirimkan email kepada orang tertentu yang kemudian memperbolehkan dia masuk ke sistem anda.

3. Pentingnya melakukan assessment terhadap insiden IT adalah melakukan proses identifikasi, menilai, mengontrol dan bahkan meminimalisir adanya risiko yang mungkin akan terjadi yang dapat membantu manajer ataupun pimpinan perusahaan ketika akan mengambil sebuah keputusan. Selain itu, dapat mengembangkan atau menciptakan strategi dalam mengelola risiko. Contoh dilakukan penilaian terhadap risiko yang terjadi document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL. Penilaian terhadap risiko merupakan gabungan proses yang terdiri dari risk analysis (analisis risiko) dan risk evaluation (evaluasi risiko). Penilaian risiko terhadap risiko yang terjadi pada document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL dilakukan untuk mengevaluasi dan mengestimasi level of risk (tingkatan risiko) dari masing-masing risiko yang telah diidentifikasi pada proses identifikasi risiko dan menetapkan acceptable level of risk (tingkatan risiko yang dapat diterima organisasi. (Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management System di PT. Jabar Telematika (JATEL).

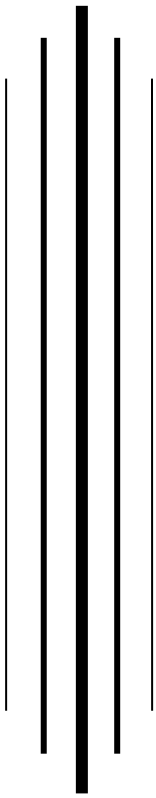
   https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjD69ms38DuAhUUfSsKHbTtDI0QFjACegQIAxAC&url=https%3A%2F%2Fmedia.neliti.com%2Fmedia%2Fpublications%2F134608-ID-analisis-manajemen-risiko-teknologi-info.pdf&usg=AOvVaw1poLZLfOMBpfGUWAilhrea

4. Disaster Recovery merupakan stretegi untuk membuat perencanaan perlindungan terhadap aset IT, karena saat ini IT sudah menjadi aset penting dalam perusahaan, aset-aset yang perlu di lindungi ini meliputi, Data, Infrastruktur IT dan Aplikasi. Kontribusi disaster recovery terhadap pengguna IT untuk pencegahan resiko dan melindungi infrastuktur dari serangan, mengenai pembuatan perencaan dan framework guna menjamin proses bisnis dapat terus berlanjut dalam situasi darurat, mengenai pemulihan cepat dari situasi darurat atau bencana agar dampak yang dihasilkan dari bencana tersebut hanya mempangaruhi organisasi atau perusahaan seminimum mungkin serta menjamin keberlangsungan proses bisnis utama.

5. Karena penerapkan Manajemen Risiko dalam lingkungan IT, merupakan hal yang sangat penting untuk di lakukan untuk menggali kejadian-kejadian dalam pelaksanaan tindakan dan kegiatan yang mungkin dapat menghambat pencapaian tujuan atau sasaran. Dengan kata lain, identifikasi risiko untuk mencari dan mendaftar risiko yang ada dan terkait dengan tujuan dan aktivitas organisasi (business process) serta mengetahui tingkat terjadinya dan dampak suatu suatu kejadian yang menghambat pencapaian tujuan atau sasaran organisasi supaya dapat dilakukan penanganan risiko secara tepat lagi. Untuk menghasilkan identifikasi risiko secara akurat, maka harus menggunakan metode yang tepat dan melibatkan para pemilik risiko (risk owner). Metode yang tepat akan menghasilkan ketepatan proses penilaian, sedangkan keterlibatan pemilik risiko diperlukan sebagai pihak yang mengerti kegiatan dan menjadi pihak yang terkena dampak atas terjadinya risiko.

UAS IT RISK MANAGEMENT

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

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?

   Seorang manajer pendanaan (fund manager) atau investor sangat jeli saat melakukan manajemen risiko karena potensi kerugian yang mungkin dialami ketika berinvestasi harus bisa diprediksi. Setelah mengetahui risiko yang mungkin terjadi, selanjutnya bisa menyusun rencana dan mengambil tindakan yang tepat untuk mengurangi nilai risiko tersebut sesuai dengan tujuan investasi. Risiko yang mungkin dihadapi dapat ditoleransi berdasarkan beberapa kategori risiko. Risiko yang menimbulkan bahaya kecil biasanya dibiarkan, sedangkan risiko yang menimbulkan bahaya besar bagi perusahaan cenderung harus dihindari atau disiapkan strategi yang terperinci untuk mengatasinya.

   IT Risk Management (Manajemen Resiko Teknologi Informasi) adalah suatu proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang digunakan oleh sebuah organisasi dan dilakukan oleh manajer IT untuk mencapai tujuan bisnis,mengurangi resiko, dan menyeimbangkan pengeluaran dalam mencapai keuntungan dan melindungi IT.

   Manajemen Resiko adalah Proses yang berlanjut. Hal ini merupakan cara perusahaan mengidentifikasi semua resiko yang mungkin terjadi yang dapat menghambat kesuksesan proyek, maka mereka harus memilih salah satu yang paling mungkin terjadi. Perusahaan harus membuat keputusan berdasarkan pengalaman mengenai kemungkinan terjadinya, data, insting dll. Awal proyek ada banyak resiko kemudian seiring proyek. Manajemen resiko harus selesai pada awal siklus proyek secara terus-menerus.

   Jika manajemen resiko diatur dengan baik, proses akan terus menerus identifikasi masalah dan resolusi, maka sistem akan mudah melengkapi sistem lain. Hal ini termasuk organisasi, perencanaan dan penganggaran, dan kontrol biaya. Adapun hal yang tidak terduga akan berkurang karena penekanan akan menjadi manajemen yang proaktif dan bukan reaktif.

   Dalam perusahaan tentunya tidak melupakan sistem manajemen resiko IT. Manajemen resiko dirancang untuk melakukan lebih dari sekedar mengidentifikasi resiko. Sistem juga harus mampu mengukur resiko dan memprediksi dampak dari resiko pada proyek. Hasilnya adalah resiko yang dapat diterima atau tidak dapat diterima. Persetujuan atau tidak dari suatu resiko biasanya tergantung pada tingkat toleransi manajer proyek untuk resiko. Di dalam manajemen resiko IT terdapat 3 proses yaitu:

   a. 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).

   b. 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. 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.

   c. 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. Adapun fungsi dari manajemen resiko IT adalah sbb:

a. Memberikan panduan untuk membantu para eksekutif dan manajemen mengajukan pertanyaan kunci, membuat lebih baik, keputusan risiko-disesuaikan lebih banyak informasi dan membimbing perusahaan mereka sehingga risiko dikelola secara efektif
b. Membantu menghemat waktu, biaya dan tenaga dengan alat untuk mengatasi risiko bisnis
c. Mengintegrasikan manajemen TI terkait risiko bisnis menjadi manajemen risiko perusahaan secara keseluruhan
d. Membantu kepemimpinan memahami risiko perusahaan dan toleransi risiko
e. Memberikan panduan praktis didorong oleh kebutuhan kepemimpinan perusahaan di seluruh dunia

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

Keamanan Teknologi Informasi adalah usaha yang dilakukan agar teknologi informasi yang digunakan baik perangkat lunak (software), perangkat keras (hardware) dan perangkat pikir (brainware) tetap berjalan sesuai dengan fungsinya. Semua perangkat tersebut harus dilindungi agar terhindar dari serangan orang yang tidak bertanggungjawab seperti hacker misalnya. Keamanan teknologi informasi disebut juga dengan dengan istilah cyber security atau information technology security (IT Security).

IT Security perlu dikelola agar teknologi yang digunakan bisa mengantarkan kepada tujuan penggunaan teknologi. Karena jika tidak maka penggunaan teknologi bisa sebaliknya menjauhkan dari tujuan. Mengelola keamanan teknologi bisa dimulai dari :

a. Mengidentifikasi risiko dari penggunaan teknologi informasi
b. Menemukan ancaman penggunaan teknologi informasi
c. Membuat kebijakan keamanan atau security policy
d. Mengontrol kebijakan yang telah dibuat.

Beberapa tahun ini aspek IT Security menjadi pokok permasalahan dalam penggunaan teknologi informasi, seolah penggunakan teknologi mempunyai dua sisi mata pedang yang bisa menguntungkan sedangkan sisi lainnya bisa menjadi kerugian pagi pengguna teknologi itu sendiri. Oleh karena itu, manajemen ini menjadi kebutuhan dalam organisasi. Di dalam manajemen dibangun kebijakan mengenai keamanan teknologi informasi dalam memaksimalkan penggunaan teknologi itu sendiri. Salah satu prinsip keamanan IT Security adalah Integrity.

Integrity atau disebut juga dengan integritas yaitu data tidak berubah dari aslinya oleh pihak yang tidak memiliki otoritas, sehingga kualitas, akurasi, dan validitas data tersebut masih terjaga. Atau dengan kata lain, integrity memastikan bahwa data yang ada benar-benar asli tidak ada yang mengubah. Data yang ada tidak dirubah baik sengaja oleh peretas atau karena tidak sengaja seperti force majuer.

Integrity dapat dilakukan dengan cara seperti:

a. Membatasi akses kontrol

Akses ke sistem dibatasi hanya pihak yang memiliki kepentingan saja. Akses kontrol dimasukkan kedalam kebijakan kemanan teknologi informasi atau security policy. Kontrol akses adalah layanan keamanan komputer yang berperan dalam mengatur pengaksesan sumber daya. Sumber daya tersebut dapat berupa berkas, software, maupun hardware. Kontrol akses ini membatasi pengguna yang akan mengakses sumber daya tersebut.

Dalam melakukan proses mediasi pada setiap permintaan ke sumber daya, dan data akan dikelola oleh sistem dengan cara menentukan apakah permintaan tersebut harus diberikan atau ditolak. Pada model kontrol akses secara tradisional akan membatasi skenario yang akan muncul, dengan memerlukan pengembangan secara terbuka di mana keputusan yang diberikan untuk melakukan akses tergantung pada sifat (atribut) dari pemohon ketimbang identitas. Pembatasan terhadap kontrol akses akan ditegakkan, walaupun itu berasal dari otoritas yang berbeda.

Fungsi kontrol akses yakni memberikan ijin kepada pengguna yang memiliki hak untuk menggunakan sumber daya yang ada. Dengan demikian, fungsi lainnya yakni mencegah pengguna maupun penyusup yang berusaha menggunakan sumber daya tersebut.

Teknik Kontrol Akses

Teknik kontrol akses yang dipilih harus cocok terahadap organisasi agar bisa memberikan tingkat keamanan yang paling maksimum. Ada beberapa teknik kontrol akses yang biasa digunakan.

Mandatory Access Control (MAC)

Mandatory Access Control (MAC) atau Mandatory kontrol akses memberikan sebuah label keamanan terhadap semua subyek dan obyek yang ada dalam sebuah sistem. Beberapa klasifikasi dari mandatory kontrol akses berdasarkan military data classification bisa dilihat pada tabel berikut ini.

Classification	Description
Unclassified	Data tidak sensitive atau classified
Sensitive but unclassified (SBU)	Data bisa menyebabkan kerugian jka tidak dicuri
Confidential	Data hanya untuk kalangan internal
Secret	Data yang bisa menyebabkan kerusakan serius pada keamanan nasional
Top Secret	Data yang bisa menyebabkan kerusakan yang parah pada keamanan nasional

Millitary Data Classification

Sedangkan yang bersifat komersial, bisa dilihat dalam tabel berikut ini.

Classification	Description
Public	Data tidak di lindungi dimanapun
Sensitive	Informasi bisa berpengaruh terhadap bisnis dan kepercayaan public jika tidak dilindungi dengan baik
Private	Informasi personal yang bisa berakibat negatif terhadap seseorang jika bocor
Confidential	Informasi perusahaan yang bisa berakibat negatif terhadap organisasi jika bocor

Ada Satu lagi metode implementasi yang umum dipakai adalah rule-based access control. Pada metode ini semua akses diberikan melalui referensi security clearance dari subyek dan security label dari obyek. Kemudian peraturan menentukan mana dari permintaan akses tersebut yang diberikan dan mana yang ditolak. Need to know property mengindiksikan sebuah subyek memerlukan akses kepada obyek untuk menyelesaikan kegiatan.

Directional Access Control (DAC)

Directional Access Control mempergunakan identitas dari subyek untuk menentukan apakah permintaan akses tersebut akan dipenuhi atau di tolak. Kontrol akses ini di desain kurang aman daripada mandatory access control tetapi merupakan desain yang paling umum dipergunakan pada berbagai sistem operasi. Metode ini lebih mudah di implementasikan dan lebih fleksibel. Setiap obyek memiliki permissions, yang menentukan user atau group yang bisa melakukan akses terhadap obyek.

Directional access control termasuk Identity-based access control dan access control list. Identity-based access control membuat keputusan untuk akses terhadap obyek berdasarkan userid atau keanggotaan group dari user yang bersangkutan. Pemilik dari obyek yang menentukan user atau group yang mana yang bisa melakukan akses terhadap obyek. Kebanyakan sistem operasi memberikan hak akses read, write and execute permisions. Untuk membuat administrasi menjadi lebih mudah maka Access Control Lists (ACLs) mengijinkan groups dari obyek, atau groups dari subyek untuk dikontrol bersama-sama. Acces Control Lists dapat memberikan hak akses terhadap group dari subyek atau memberikan hak kepada akses group dari subyek kepada obyek tertentu.

Non-discretionary Access Control

Ini merupakan desain kontrol akses yang ketiga. Biasanya menggunakan role dari subyek atau kegiatan yang di assigned kepada sebuah subyek, untuk menerima atau menolak akses. Non-discretionary access control disebut juga roled-based acces control atau task base access control. Tipe kontrol akses ini cocok dipakai pada kasus high turnover atau reassginments. Ketika security di asosiasikan kedalam sebuah role atau task, mengganti orang yang mengerjakan tugas membuat security administration lebih mudah.

Lattice-based access control adalah salah satu variasi dari desain non-discretionary access control. Disamping mengasosiasikan beberapa kontrol akses dengan task atau role yang spesifik, masing-masing hubungan antara subyek dan obyek memiliki beberapa pasang batasan. Batasan akses ini yang mendifinisikan peraturan dan kondisi yang mengijinkan mengakses sebuah obyek. Pada kebanyakan kasus, batas akses mendefinisikan batas atas dan batas bawah yang menyatakan klasifikasi dari keamanan dan label.

Langkah berikutnya dari organisasi setelah melakukan desain terhadap kontrol akses adalah menentukan access control administration. Acces control administration bisa di

implementasikan baik centralized atau decentralized. Pilihan terbaik dalam melakukan administrasi tergantung dari kebutuhan dari origanisasi dan sensitivitas informasi yang disimpan dalam sistem komputer.

Centralized Access Control

Centralized access control administration memerlukan sebuah pusat keamanan yang bisa menentukan apakah sebuah permintaan akan disetujui atau ditolak. Pendekatan ini sangat mudah karena obyek hanya di pelihara pada lokasi yang tunggal. Salah satu kelemahannya adalah central access control bisa menjadi sebuah single point of failure. Jika central access control rusak, maka semua obyek tidak akan bisa diakses. Dampak negatif yang lainnya adalah dalam masalah perfomance, jika sistem tidak bisa memmenuhi semua permintaan dari user. Anda dapat memilih beberapa paket yang biasa dipakai dalam mengimplementasikan administrasi terhadap kontrol akses.

Remote Authentication Dial-In User Service (RADIUS) menyediakan kontrol akses kepada user yang melakukan dial-in. User di validasi berdasarkan list dari user yang ada di RADIUS server. Anda bisa melakukan hang-up dan memanggil user kembali melalui nomor telepon yang ada di server. Contoh lain dari Centralized Access Control adalah Chalenge Handshake Authentication Protocol (CHAP). CHAP menampilkan tantangan ketika user meminta akses. Jika user merespon tantangan tersebut dengan benar maka user tersebut akan diberikan hak CHAP mengembangkan keamanannya dengan melakukan enkripsi selama pertukaran pesan.

Centralized Access Control untuk aplikasi network bisa menggunakan TACACS (Terminal Access Controller Acess Control System). TACACS menyediakan services umum untuk melakukan Authentication dan Authorization.

Decentralized Access Control Decentralized Access Control meletakan tanggung jawab dari lebih dekat terhadap obyek. Pendekatan ini memerlukan lebih banyak administerasi daripada centralized access control karena sebuah obyek mungkin saja memerlukan kondisi yang sangat aman pada lokasi tertentu. Tapi hal ini bisa lebih stabil karena tidak ada Single Point Of Failure. Decentralized Access Control biasanya diimplementasikan memakai security domain. Security domain adalah bagian sebuah kepercayaan, atau koleksi dari obyek dan subyek, yang mendefinisikan access rule dan permisions. Subyek harus termasuk dalam domain tersebut. Pendekatan ini bisa memudahkan untuk mengeluarkan subyek yang dicurigai, tetapi bisa membuat administrasi secara umum lebih sulit karena berbagai macam variasi dari peraturan keamanan.

b. Membuat otentifikasi

Elemen user interface yang pertama kali ditemui kebanyakan subjek ketika mengakses sistem informasi adalah identifikasi dan otentikasi. Tahap identifikasi memperkenankan subjek mengklaim sebagai entitas tertentu dengan menunjukkan bukti-bukti identitas. Bukti-bukti tersebut dapat sesederhana user ID atau nomer PIN, atau yang lebih kompleks seperti atribut fisik. Setelah subjek mengklaim suatu identitas, sistem memvalidasi apakah user tersebut terdaftar dalam user database dan membuktikan bahwa subjek tesebut adalah benar-benar sebagai entitas yang diklaimnya. Tahap otentikasi meminta subjek menujukkan informasi tambahan yang berkesusaian dengan informasi tentang subjek tesebut yang telah disimpan. Dua tahap ini sering disebut dengan otentikasi dua faktor, yang memberikan proteksi terhadap subjek yang tidak memiliki otoritas untuk mengakses sistem. Setelah subjek diotentikasi, sistem kontrol akses mengevaluasi hak dan izin subjek untuk mengabulkan atau menolak permintaan akses terhadap objek. Tahap ini disebut dengan tahap otorisasi.

Ada tiga kategori/tipe umum dari informasi otentikasi. Pratek pengamanan yang baik biasanya membuat tahap identifikasi dan otentikasinya memerlukan input setidaknya dari dua tipe berbeda. Tiga tipe umum data otentikasi dijelaskan dalam Tabel berikut ini.

Authentication Type	Description	Examples
Type 1	What you know	Password, passphrase, PIN, lock combination
Type 2	What you have	Smart card, token device
Type 3	What you are	Biometrics—fingerprint, palm print, retina/iris pattern, voice pattern

Tipe otentikasi yang paling umum dan paling mudah untuk di implementasikan adalah otentikasi tipe 1. Yang dilakukan adalah meminta subjek membuat password passphrase, atau nomer PIN. Alternatif lain adalah menyediakannya untuk user. Kesulitan dalam otentikasi tipe 1 adalah perlunya mendorong subjek untuk membuat frase yang sangat sulit diterka oleh orang lain, namun tidak terlalu rumit sehingga sulit untuk diingat. Password (frase atau PIN) yang sulit diingat akan mengurangi nilai dari password itu sendiri. Hal tersebut dapat terjadi bila administrator terlalu sering mmerlukan penggantian password sehingga user kesulitan untuk mengingat password terbaru. Jadi, yang disarankan adalah menjaga password secara rahasia dan aman. Aturan-aturan berikut ini adalah petunjuk yang baik untuk membuat password yang aman.

- Password setidak memiliki panjang 6 karakter.
- Password setidaknya mengandung sebuah angka atau karakter tanda baca.
- Tidak menggunakan kosakata atau kombinasi kosakata.
- Tidak menggunakan data pribadi, seperti tanggal kelahiran, nama anggota keluarga atau binatang peliharaan, atau lagu atau hobi favorit.
- Tidak sesekali menuliskan password.
- Membuat password yang mudah diingat tetapi sulit diterka

Data otentikasi tipe 2 lebih rumit untuk dilakukan karena subjek perlu membawa suatu alat atau sejenisnya. Alat tersebut umumnya perangkat eleltronik yang menghasilkan suatu nilai yang bersifat sensitif terhadap waktu atau suatu jawaban untuk diinput. Meskipun otentikasi tipe 2 lebih rumit, tipe ini hampir selalu lebih aman dibandingkan dengan otentikasi tipe 1.

Otentikasi tipe 3, atau biometrics adalah yang paling canggih. Biometric menggambarkan pendeteksian dan pengklasifikasian dari atribut fisik. Terdapat banyak teknik biometric yang berbeda, diantaranya:

- Pembacaan sidik jari/telapak tangan
- Geometri tangan
- Pembacaan retina/iris
- Pengenalan suara
- Dinamika tanda tangan

Karena kerumitannya, biometric adalah tipe otentikasi yang paling mahal untuk diimplementasikan. Tipe ini juga lebih sulit untuk dipelihara karena sifat ketidaksempurnaan dari analisis biometric. Dianjurkan untuk berhati-hati beberapa masalahmasalah utama dari eror-eror biometric. Pertama, sistem mungkin menolak subjek yang memiliki otoritas. Ukuran kesalahan semacam ini disebut dengan false rejection rate (FRR). Di sisi lain, sistem biometric

mungkin menerima subjek yang salah. Ukuran kesalahan semacam ini disebut dengan false acception rate (FAR). Yang menjadi masalah adalah ketika sensitifitas sistem biometric diatur untuk menurunkan FRR, maka FAR meningkat. Begitu juga berlaku sebaliknya. Posisi pengaturan yang terbaik adalah bila nilai FRR dan FAR seimbang, ini terjadi pada crossover error rate (CER).

Single Sign-On

Semakin banyak informasi, atau faktor, yang diminta dari subjek, semakin menjamin bahwa subjek adalah benar-benar entitas yang diklaimnya. Oleh karenanya, otetikasi dua faktor lebih aman dari otentikasi faktor tunggal. Masalah yang timbul adalah bila subjek ingin mengakses beberapa sumber daya pada sistem yang berbeda, subjek tersebut mungkin diminta untuk memberikan informasi identifikasi dan otentikasi pada masing-masing sistem yang berbeda. Hal semacam ini dengan cepat menjadi sesuatu yang membosankan. Sistem Single Sign-On (SSO) menghindari login ganda dengan cara mengidentifikasi subjek secara ketat dan memperkenankan informasi otentikasi untuk digunakan dalam sistem atau kelompok sistem yang terpercaya. User lebih menyukai SSO, namun administrator memiliki banyak tugas tambahan yang harus dilakukan. Perlu perhatian ekstra untuk menjamin bukti-bukti otentikasi tidak tidak tersebar dan tidak disadap ketika melintasi jaringan. Beberapa sistem SSO yang baik kini telah digunakan. Tidak penting untuk memahami setiap sistem SSO secara detail. Konsep-konsep penting dan kesulitan-kesulitannya cukup umum bagi semua produk SSO.

Kerberos

Sistem Kerberos berasal dari Athena, proyek Massachusetts Institute of Technology (MIT). Kerberos memberikan proteksi baik terhadap otentikasi dan pesan. Kerberos menggunakan kriptografi kunci simetris (kedua sisi memiliki kunci yang sama) untuk meng-enkripsi pesan. Fitur dari enkripsi memberikan keamanan bersifat end-to-end, yang berarti bahwa mesin yang berada di antara mesin asal dan target tidak dapat melihat isi dari pesan. Kerberos berkembang populer untuk digunakan dalam sistem yang terdistribusi. Walaupun dapat bekerja baik dalam lingkungan yang terdistribusi, kerberos sendiri menggunakan server tersentralisasi untuk menyimpan kunci-munci kriptografi.

Kerberos mencakup sebuah repositori data dan proses otentikasi. Key Distribution Center (KDC) berada di pusat dari Kerberos. KDC menyimpan semua kunci kriptografi dari subjek dan objek. KDC memiliki peran untuk memelihara dan mendistribusikan kunci-kunci tersebut, juga menyediakan layanan otentikasi (AS, Authentication Service). Ketika KDC menerima permintaan akses terhadap suatu objek, KDC memanggil AS untuk melakukan otentikasi terhadap subjek dan permintaannya. Bila permintaan subjek diotentikasi, AS membuat tiket akses yang berisi kunci bagi subjek dan objek kemudian mendistribusikan kunci tersebut ke subjek dan objek. Berikut adalah langkah-langkah dasar dalam siklus permintaan akses Kerberos:

- Subjek melakukan permintaan akses terhadap suatu objek. Software Kerberos subjek meminta user ID, dan mengirim user ID tersebut bersama permnitaan subjek ke KDC.
- KDC memanggil AS untuk melakukan otentikasi terhadap subjek dan objek.
- Jika otentikasi diberikan, KDC mengirimkan sebuah kunci sesi yang ter-enkripsi ke mesin subjek dan objek.
- Software Kerberos klien subjek meminta password subjek dan menggunakannya, bersama dengan kunci rahasia subjek, untuk men-dekripsi kunci sesi.
- Kemudian subjek mengirim permintaan akses bersama dengan kunci sesi ke objek.

- Objek men-dekripsi kunci sesi yang diterima dari KDC dan membandingkannya dengan kunci sesi yang diterimanya bersamam permintaan akses.
- Jika kedua kunci sesi bersesuaian, akses dikabulkan. Sifat tersentralisasi dan KDC menampakkan satu dari kelemahan utama Kerberos: KDC merupakan titik tunggal kegagalan.

Kegagalan KDC berarti kegagalan akses objek. KDC juga dapat menjadi bottleneck kinerja bagi mesin berbeban besar. Juga, terdapat sedikit peluang saat kunci sesi berada dalan mesin klien. Terbuka kemungkinan bagi penyusup untuk menanngkap kunci ini dan mendapatkan akses terhadap sumber daya tanpa terotorisasi. Meskipun meiliki beberapa kekurangan, Kerberos merupakan contoh yang baik dari sistem SSO dan telah mendapat sambutan luas.

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan)

   Dalam melakukan manajemen resiko IT tentunya ada 3 tahap yang harus dilakukan. Tahap tersebut risk assessment, risk mitigation serta evaluation. 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.
   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.
   Setelah melakukan identifikasi risiko, maka tahap berikutnya adalah pengukuran risiko dengan cara melihat potensial terjadinya seberapa besar severity (kerusakan) dan probabilitas terjadinya risiko tersebut. Penentuan probabilitas terjadinya suatu event sangatlah subyektif dan lebih berdasarkan nalar dan pengalaman. Beberapa risiko memang mudah untuk diukur, namun sangatlah sulit untuk memastikan probabilitas suatu kejadian yang sangat jarang terjadi. Sehingga, pada tahap ini sangatlah penting untuk menentukan dugaan yang terbaik supaya nantinya kita dapat memprioritaskan dengan baik dalam implementasi perencanaan manajemen risiko. Kesulitan dalam pengukuran risiko adalah menentukan kemungkinan terjadi suatu risiko karena informasi statistik tidak selalu tersedia untuk beberapa risiko tertentu. Selain itu, mengevaluasi dampak severity (kerusakan) seringkali cukup sulit untuk asset immaterial. Hasil akhir dari analisis risiko adalah penentuan risiko (contoh: tingkat bahaya dan kemungkinan dari bahaya yang terjadi).
   Berikut ada salah satu penerapan risk assessment pada perusahaan PT JATEL berdasarkan Husein (2015). Pada proses ini dilakukan penilaian terhadap risiko yang terjadi document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL. Penilaian terhadap risiko merupakan gabungan proses yang terdiri dari risk analysis (analisis risiko) dan risk evaluation (evaluasi risiko). Penilaian risiko terhadap risiko yang terjadi pada document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL

dilakukan untuk mengevaluasi dan mengestimasi level of risk (tingkatan risiko) dari masing-masing risiko yang telah diidentifikasi pada proses identifikasi risiko dan menetapkan acceptable level of risk (tingkatan risiko yang dapat diterima) organisasi.

1. Risk Analysis
   Analisis risiko dilakukan untuk menentukan seberapa sering risiko pada document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL dapat terjadi dan seberapa besar dampak yang dihasilkan apabila risiko tersebut terjadi.

- Bow-tie Analysis Bow-tie Analysis dilakukan agar proses analisis terhadap risiko menghasilkan recovery (pemulihan) dan control (kontrol).

TABEL IV
TABEL *BOW-TIE ANALYSIS* PADA *EXTERNAL ATTACKS*

Threats	Impact/ Consequences	Recovery	Control
Ping Flooding *Bandwidth Flooding*	*Bandwidth Consuming.* Aplikasi tidak dapat diakses. Akses dari IP yang tidak dikenal. *Network Congestion.*	Menghentikan *packet data* dari IP yang tidak dikenal. Memblokir akses dari IP yang tidak dikenal. Melakukan *load balancing.* Mengalokasikan *bandwidth.*	*Firewall.* *Load Balancer.* *Network Attach Storage* (NAS). *Demiliterized Zone* (DMZ). *Virtual Private Network* (VPN).
SQL Injection	Manipulasi Data. Pencurian Data. *User Input Injection.* *Cookies*	*Restore Data.* Mengubah *statement* pemograman. *Session.*	*Firewall.* Enkripsi Data. Merubah statement pemograman, *Session.*

Threats	Impact/ Consequences	Recovery	Control
	Injection.		
Content Tempering	*Tempered Content.*	*Restore Data.* Mengulang *session data.*	

Pada Tabel IV diketahui bahwa terdapat empat ancaman yang dapat menyebabkan kemungkinan terjadinya external attacks pada document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL, yaitu ping flooding, bandwidth flooding, SQL Injection, dan Content Tempering. Pada tabel yang sama dapat juga dilihat impact/consequences, recovery, dan control untuk external attacks.

- Klasifikasi Impact/Consequences Pada Kelompok Risiko
  Pada tahap ini dilakukan klasifikasi impact/ consequences tiap kelompok risiko pada sumber daya IT yang mendukung penerapan document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL.

TABEL V
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *APPLICATION*

Kelompok Risiko	*Threats*	*Impact/ Consequences*	Klasifikasi
External Attacks	*Ping Flooding*	*Bandwidth Consuming*	*Performance*
		Aplikasi tidak dapat diakses	*Availability*
	Bandwidth Flooding	Akses dari IP yang tidak dikenal	*Security*
		Network Congestion	*Performance*
	SQL Injection	Manipulasi Data	*Security*
		Pencurian Data	*Security*
		User Input Injection	*Security*
		Cookies Injection	*Security*
	Content Tempering	*Tempered Content*	*Security*
Malicious Code	*Trojan Horses*	*Data Loss*	*Availability*
		Backdoor Access	*Security*
		Network Usage	*Performance*
		Adanya *Backdoor Programing*	*Security*
	Worms	Replikasi Data	*Security*
		Network Traffic	*Performance*
	Viruses	Replikasi Data	*Security*
		Manipulasi Data	*Security*
		Infected Areas	*Security*
	Phising	Pencurian Data	*Security*
Network Congestion	*Slow Network Throughtput*	Layanan Terganggu	*Performance*
		Aplikasi tidak bias diakses	*Availability*
		Bottleneck	*Performance*
System Crash	*Application Crashes*	Aplikasi tidak dapat digunakan	*Availability*
		Data Loss	*Availability*
	Web Server Crashes	Aplikasi/ web server tidak dapat diakses	*Availability*
	Operation System Crashes	*Kernel Panic*	*Availability*

TABEL VI
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *INFORMATION*

Kelompok Risiko	*Threats*	*Impact/ Consequences*	Klasifikasi
Database Failure	*Statement Failure*	*Looping*	*Performance*
		Memory Penuh	*Performance*
		Data tidak tersimpan	*Compliance*
	System Crash	*Error Connection Database*	*Availability*
		Application Crashes	*Availability*
		Web Server Crashes	*Availability*
		Operation System Crashes	*Availability*
	Human Error	Kesalahan Statement	*Performance*
		Kesalahan Prosedur yang menyebabkan kerusakan	*Compliance*
	Network Failure	Data tidak tersimpan karena kerusakan *network interface controller*	*Compliance*
		Error Connection Database	*Availability*
	Media Failure	Data tidak tersimpan karena ekstensi file tidak di *support*	*Compliance*
		Error Connection Database	*Availability*
	Disk Failure	*Bad Hardisk Sector*	*Availability*
	Corrupted File	*Corrupted Data*	*Availability*
Data/ Document Fraud	*Content Tempering*	*Tempered Content*	*Availability*
	Content Forging	*Forged Content*	*Availability*

Kelompok Risiko	*Threats*	*Impact/ Consequences*	Klasifikasi
		Data Loss	*Availability*
Hardware Failure	*Electrical Dischagrge*	Korsleting	*Availability*
		Kerusakan pada hardware/ modul	*Availability*
		Sengatan Listrik	*Compliance*
	Short Circuit	Kerusakan pada hardware/ modul	*Availability*
	Power Surges	*Server Interupts*	*Availability*
		Hard Bad Sector	*Availability*
	Overheating	Hardware tidak aktif	*Availability*
		Corrupted Data	*Availability*
		Data Loss	*Availability*
	Bad Hardisk Sector	*Hard Bad Sector*	*Availability*
		Soft Bad Sector	*Performance*
		Corrupted Data	*Availability*
		Data Loss	*Availability*
	Corrupted File	*Corrupted Data*	*Availability*
		Data Loss	*Availability*
	Human Error	Kerusakan Hardware	*Availability*
		Data loss	*Availability*
Power Outage	*Power Cut/ Power Blackout/ Power Failure*	Ketidak tersediaan Infrastruktur	*Availability*
Force Majure	Bencana Alam	Kerusakan Infrastruktur	*Availability*
		Kerusakan Hardware	*Availability*
		Data Loss	*Availability*
Disgruntled Employees	*Unauthorized Access*	Manipulasi Data	*Security*
		Perubahan Konfigurasi	*Security*
	Penyebaran Informasi	Tersebarnya Informasi Rahasia	*Compliance*
	Lemahnya Pengetahuan Terhadap Aplikasi	*Output* dari aplikasi tidak optimal	*Performance*

TABEL VIII
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *PEOPLE*

Kelompok Risiko	Threats	Impact/ Consequences	Klasifikasi
Inappropriate Access	*Unauthorized Access/ Man in The Middle*	Pencurian Data	*Security*
		Manipulasi Data	*Security*
		Akses yang tidak diinginkan	*Security*
Abuse of Position of Trust	*Inappropriate Access*	Manipulasi Data	*Security*
		Perubahan Konfigurasi	*Security*
	Content Tempering	*Tempered Content*	*Security*
	Content Forging	*Forged Content*	*Security*
	Penyebaran	Tersebarnya	*Compliance*

TABEL IX
NILAI PADA *LIKELIHOOD*

Likelihood		Frekuensi per Tahun
Rating	Kriteria	
1	*Rare*	≤ 5 Kejadian
2	*Unlikely*	6 – 10 Kejadian
3	*Possible*	11 – 20 Kejadian
4	*Likely*	21 – 40 Kejadian
5	*Almost Certain*	≥ 41 kejadian

TABEL X
NILAI PADA *IMPACT*

Impact		Deskripsi
Rating	Kriteria	
1	*Insignificant*	Dampak mungkin diabaikan dengan aman.
2	*Minor*	Dampak kecil dan dapat diatasi dengan prosedur sederhana
3	*Moderate*	Dampak tergolong besar, namun dapat dikelola dengan menggunakan prosedur tertentu
4	*Major*	Dampak besar, berpotensi pada *financial cost* dan terhambatnya kinerja organisasi
5	*Catastrophic*	Dampak ekstrim, berpotensi pada *large financial cost* dan terhentinya kinerja organisasi, serta dampak pada reputasi organisasi

TABEL XI
IDENTIFIKASI *LIKELIHOOD* DAN *IMPACT*

No	Identifikasi Risiko	*Likelihood*	*Impact*
1	*External Attacks*	*Rare*	*Moderate*
2	*Malicious Code*	*Rare*	*Minor*
3	*Physical Damage*	*Rare*	*Moderate*
4	*Inappropriate Access*	*Rare*	*Major*
5	*Hardware Failure*	*Rare*	*Minor*
6	*Power Outages*	*Possible*	*Moderate*
7	*Database Failure*	*Rare*	*Moderate*
8	*Force Majure*	*Rare*	*Catastrophic*
9	*Network Congestion*	*Possible*	*Moderate*
10	*System Crash*	*Rare*	*Minor*
11	*Data/Documen Fraud*	*Rare*	*Major*
12	*Abuse of Position of Trust*	*Rare*	*Major*
13	*Disgruntled Employees*	*Unlikely*	*Minor*

TABEL XII
PENILAIAN *LIKELIHOOD* DAN *IMPACT*

No	Identifikasi Risiko	*Likelihood*	*Impact*
1	*External Attacks*	1	3
2	*Malicious Code*	1	2
3	*Physical Damage*	1	3
4	*Inappropriate Access*	1	4
5	*Hardware Failure*	1	2
6	*Power Outages*	3	3
7	*Database Failure*	1	3
8	*Force Majure*	1	5
9	*Network Congestion*	3	3
10	*System Crash*	1	2
11	*Data/Documen Fraud*	1	4
12	*Abuse of Position of Trust*	1	4
13	*Disgruntled Employees*	1	2

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimasuk dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi resiko terhadap penggunaan IT bagi organisasi?

   Teknologi informasi saat ini sudah menjadi kebutuhan setiap perusahaan, secara umum teknologi informasi dapat diterapkan di segala bidang bisnis, baik dari bidang pelayanan masyarakat, rumah sakit, pendidikan, pemerintahan, swasta dll. Setiap bisnis yang menggunakan teknologi informasi secara efektif mereka akan memproses informasi dengan cepat.

   Sebagian besar perusahaan modern sudah menggunakan teknologi informasi untuk membantu kinerja di dalam operasional bisnis mereka, sebagai contoh dalam penerapan ini adalah penggunaan Sistem Informasi Bisnis, dimana sebuah proses bisnis perusahaan bergantung pada sebuah sistem informasi. perusahaan perlu merencanakan kelangsungan operasional bisnis mereka dengan membuat stretegi yang disebut dengan IT Disaster Recovery Plan.

   IT Disaster Recovery Plan merupakan stretegi untuk membuat perencanaan perlindungan terhadap aset IT, karena saat ini IT sudah menjadi aset penting dalam perusahaan, aset-aset yang perlu di lindungi ini meliputi, Data, Infrastruktur IT, Aplikasi.

   Perusahaan besar dan kecil sama-sama memiliki kebutuhan umum seperti membuat dan mengelola informasi data secara elekronik. Banyak data yang penting dan juga beberapa data

yang sangat penting untuk kelangsungan hidup dan melanjutkan operasi bisnis dalam perusahaan.
Dampak dari kehilangan data ini bisa disebabkan oleh beberapa faktor seperti : kerusakan hardware, kesalahan manusia, hacking atau malware. Sehingga tindakan untuk melakukan backup data dan pemulihan informasi elektronik ini sangat penting.

IT Recovery Strategies

Strategi Pemulihan yang harus dikembangkan ini bertujuan untuk memulihkan aset perusahaan dalam lingkup infrastruktur IT diantaranya meliputi aplikasi, data dan sistem informasi yang termasuk diantaranya infrastruktur jaringan, server, desktop, laptop, dan internet. Prioritas utama dalam strategi untuk pemulihan ini harus konsisten dengan prioritas sebuah fungsi bisnis proses didalam perusahaan. Sumber daya TI yang dibutuhkan dalam mendukung fungsi bisnis ini adalah dengan cara mengidentifikasi waktu dan proses. Waktu pemulihan untuk sumber daya TI harus sesuai dengan tujuan bisnis proses perusahaan yang sangat tergantung pada sumber daya TI.
Di dalam Sistem teknologi informasi memliki suatu komponen yang saling terkait diantaranya perangkat keras, perangkat lunak, data dan konektivitas. Tanpa salah satu komponen tersebut, sistem tidak dapat berjalan. Oleh karena itu, strategi pemulihan harus dikembangkan untuk mengantisipasi hilangnya satu atau lebih komponen sistem berikut :

- Lingkungan ruang komputer (ruang komputer aman dengan pengatur suhu, AC dan UPS, dll)
- Hardware (jaringan, server, komputer desktop dan laptop, Wireless & router) Konektivitas ke penyedia layanan (fiber, kabel, wireless, dll)
- Aplikasi perangkat lunak (pertukaran data elektronik, surat elektronik, manajemen sumber daya perusahaan, produktivitas kantor, dll)
- Data dan restorasi

Beberapa aplikasi bisnis tidak bisa mentolerir downtime. Mereka memanfaatkan data center yang mampu menangani semua kebutuhan pengolahan data yang berjalan secara paralel dengan memanfaatkan data mirroring atau sinkronisasi antara dua data-center. Ini merupakan solusi yang sangat mahal dan hanya perusahaan besar mampu mengeluarkan biaya untuk ini. Namun, ada solusi lain yang tersedia untuk lingkup usaha kecil menengah untuk melindungi aplikasi bisnis mereka.

Internal Recovery Strategies

Banyak perusahaan memiliki akses ke lebih dari satu fasilitas. Dengan memanfaatkan Hardware alternatif yang dapat dikonfigurasi untuk perangkat lunak aplikasi yang serupa bila diperlukan. Dengan asumsi data yang didukung berada luar lokasi atau data mirroring antara dua lokasi, sehingga jika terjadi bencana, data dapat segera dipulihkan kembali di lokasi alternatif agar operasional dapat berjalan kembali.

Vendor Supported IT Recovery Strategies

Ada vendor yang menyediakan dukungan penuh terhadap solusi IT Disaster Recovery, dalam hal ini vendor biasanya menyediakan layanan perangkat lunak, hardware dan co-location server di dalam sebuah data-center yang secara umum di dalamnya terdapat hardware software dan konektivitas serta fasilitas keamanan yang diberikan untuk melindungi sistem informasi, aplikasi dan data terhadap aktifitas luar seperti hacking dan malware, data center ini biasanya telah memenuhi standar data center tinggi. Sehingga tingkat ketersediaan layananya juga tinggi. Layanan-layanan yang dapat di manfaatkan dari vendor ini diantaranya : Cloud, VPS, Hosting, Co-Location.

Mengembangkan Perencanaan IT Disaster Recovery

Sebuah Bisnis harus dapat mengembangkan rencana pemulihan bencana terhadap aset TI. Yang dimulai dengan menyusun inventarisasi perangkat keras (misalnya server, desktop, laptop, dll), aplikasi perangkat lunak dan data. Rencana tersebut harus mencakup strategi untuk memastikan bahwa semua mendukung informasi penting.

Mengidentifikasi aplikasi perangkat lunak dan data penting serta hardware yang dibutuhkan untuk menjalankannya. Yang dapat digunakan untuk membantu mereplikasi konfigurasi ke hardware baru. memastikan bahwa salinan program perangkat lunak yang tersedia untuk memungkinkan instalasi ulang pada peralatan pengganti. Dengan memprioritaskan hardware dan software pemulihan.

Mendokumentasikan perencanaan pemulihan IT dari bencana sebagai bagian dari rencana kesinambungan bisnis. Menguji rencana berkala untuk memastikan bahwa strategi pemulihan ini dapat bekerja.

Backup Data

Perusahaan secara berkala akan menghasilkan sejumlah data atau file yang berubah sepanjang hari, dan peluang terjadinya kegagalan hardware ini, dapat menyebabkan data hilang. Hal ini secara signifikan dapat mengakibatkan terhambatnya proses bisnis di dalam perusahaan.

Backup data harus menjadi bagian terpenting dari rencana untuk pemulihan dari bencana yang akan terjadi. Dengan mengembangkan strategi ini, backup data dapat di mulai dari mengidentifikasi data apa saja yang harus di backup, membuat penjadwalan dan melakukan backup secara berkala kemudian memvalidasi keakuratan data yang di dukung.

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standard yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

   Kerangka kerja manajemen risiko ISO 31000:2009 Risk Management – Principles and Guidelines diawali dengan pemberian mandat dan komitmen. Pemberian mandat dan komitmen tersebut merupakan hal yang sangat penting karena menentukan akuntabilitas, kewenangan, dan kapabilitas dari pelaku manajemen risiko. Berikut ini hal – hal penting yang harus dilakukan pada pemberian mandat dan komitmen, antara lain membuat dan menyetujui kebijakan manajemen risiko, menyesuaikan indikator kinerja manajemen risiko dengan indikator kinerja organisasi atau perusahaan, menyesuaikan kultur organisasi dengan nilai – nilai manajemen risiko, menyesuaikan sasaran manajemen risiko dengan sasaran strategis organisasi atau perusahaan, memberikan kejelasan peran dan tanggung jawab, menyesuaikan kerangka kerja manajemen risiko dengan kebutuhan organisasi atau perusahaan.

   Sesudah diawali dengan pemberian mandat dan komitmen, kerangka kerja ISO 31000: 2009 dilanjutkan dengan kerangka implementasi "Plan, Do, Check, Act", antara lain dengan melakukan perencanaan kerangka kerja manajemen risiko, penerapan manajemen risiko, pengawasan dan peninjauan terhadap kerangka kerja manajemen risiko, dan perbaikan kerangka kerja manajemen risiko secara berkesinambungan. Perencanaan kerangka kerja manajemen risiko mencakup pemahaman mengenai organisasi atau perusahaan dan konteksnya, menetapkan kebijakan manajemen risiko, menetapkan akuntabilitas manajemen risiko, mengintegrasikan manajemen risiko ke dalam proses bisnis organisasi atau perusahaan, alokasi sumber daya manajemen risiko, dan menetapkan mekanisme komunikasi internal dan eksternal. Setelah melakukan perencanaan kerangka kerja, maka dilakukan penerapan proses manajemen risiko. Dalam penerapan manajemen risiko, perlu dilakukan monitoring

dan review terhadap kerangka kerja manajemen risiko. Setelah itu, kerangka kerja manajemen risiko perlu diperbaiki secara berkelanjutan untuk memfasilitasi perubahan yang terjadi pada konteks internal dan eksternal organisasi atau perusahaan. Proses – proses tersebut kemudian berulang kembali untuk memastikan adanya kerangka kerja manajemen risiko yang mengalami perbaikan berkesinambungan dan dapat menghasilkan penerapan manajemen risiko yang andal.

Proses manajemen risiko merupakan kegiatan kritikal dalam manajemen risiko, karena merupakan penerapan prinsip dan kerangka kerja yang telah dibangun. Proses manajemen risiko itu sendiri terdiri dari tiga proses besar, yaitu :

a. Proses pertama, penetapan konteks (establishing the context). Proses ini bertujuan untuk mengidentifikasi dan mengungkapkan sasaran organisasi, lingkungan dimana sasaran hendak dicapai, stakeholders yang berkepentingan, dan keberagaman kriteria risiko, dimana hal – hal ini akan membantu mengungkapkan dan menilai sifat dan kompleksitas dari risiko. Terdapat empat konteks yang perlu ditentukan dalam penetapan konteks, yaitu konteks internal, konteks eksternal, konteks manajemen risiko, dan kriteria risiko. Dimana konteks internal memperhatikan sisi internal organisasi yaitu struktur organisasi, kultur dalam organisasi, dan hal – hal lain yang dapat mempengaruhi pencapaian sasaran organisasi. Konteks eksternal mendefinisikan sisi eksternal organisasi yaitu pesaing, otoritas, perkembangan teknologi, dan hal – hal lain yang dapat mempengaruhi pencapaian sasaran organisasi. Konteks manajemen risiko memperhatikan bagaimana manajemen risiko diberlakukan dan bagaimana hal tersebut akan diterapkan di masa yang akan datang. Terakhir, dalam pembentukan manajemen risiko organisasi perlu mendefinisikan parameter yang disepakati bersama untuk digunakan sebagai kriteria risiko.
b. Proses kedua, penilaian risiko (risk assessment), terdiri dari identifikasi risiko, yaitu mengidentifikasi risiko apa saja yang dapat mempengaruhi pencapaian sasaran organisasi. Analisis risiko, yaitu menganalisis kemungkinan dan dampak dari risiko yang telah diidentifikasi. Dan evaluasi risiko, yaitu membandingkan hasil analisis risiko dengan kriteria risiko untuk menentukan bagaimana penanganan risiko yang akan diterapkan.
c. Proses ketiga, penanganan risiko (risk treatment). Dalam menghadapi risiko terdapat empat penanganan yang dapat dilakukan oleh organisasi atau perusahaan, antara lain menghindari risiko (risk avoidance), mitigasi risiko (risk reduction), dapat dilakukan dengan mengurangi kemungkinan atau dampak. Transfer risiko kepada pihak ketiga (risk sharing) dan terakhir menerima risiko (risk acceptance).

Keberhasilan penerapan manajemen risiko bergantung pada keefektifan kerangka kerja manajemen untuk menyediakan dasar yang dapat diterapkan pada keseluruhan organisasi atau perusahaan pada seluruh tingkatan. Kerangka kerja membantu menangani risiko secara efektif melalui penerapan proses manajemen risiko pada berbagai tingkatan dan dalam konteks spesifik organisasi atau perusahaan. Kerangka kerja memastikan informasi tentang risiko yang diturunkan dari proses manajemen risiko dilaporkan secara layak dan digunakan sebagai dasar pengambilan keputusan serta akuntabilitas pada seluruh tingkatan organisasi atau perusahaan.

DAFTAR PUSTAKA

http://ftp.gunadarma.ac.id/linux/docs/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/126/126M-02-final2.0-access-control-systems.pdf

https://aliyhafiz.com/keamanan-teknologi-informasi/#2_Integrity

https://desnet.id/it-disaster-recovery-plan/#:~:text=IT%20Disaster%20Recovery%20Plan%20merupakan,Data%2C%20Infrastruktur%20IT%2C%20Aplikasi.

https://multiglobalunity.com/penerapan-manajemen-resiko/

https://sis.binus.ac.id/2019/04/08/it-risk-management/

https://toghr.com/it-risk-management-sangat-penting/

https://www.kompasiana.com/endixdr/5e7ed1aad541df06be5f7362/pentingnya-risk-management-dalam-perusahaan?page=all#sectionall

Husein, G.M., Imbar, R.V., 2015, Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management Sustem di PT. Jabar Telematika (JATEL), Jurnal Teknik Informatika dan Sistem Informasi Vol 1. No.2.

UAS IT RISK MANAGEMENT & DISASTER RECOVERY

Nama : Isti Maátun Nasichah

NPM : 192420051

1. Mengapa IT Risk Management penting diterapkan dalam suatu organisasi?
   Jawab :

   Penerapan teknologi informasi sangatah berkembang, dan berperan penting dalam dunia bisnis. Pada perusahaan, teknologi informasi tidak hanya diterapkan pada operasional saja tetapi juga proses pengambilan keputusan oleh *executive management*. Oleh karena itu, teknologi informasi merupakan hal yang harus diperhatikan dan dikelola dengan baik oleh perusahaan untuk mempertahankan bisnis yang dijalankan. Dibalik keuntungan yang diberikan, terdapat kekurangan yaitu risiko yang ditimbulkan saat menggunakan teknologi informasi yang dapat mengakibatkan kerugian. Risiko akan selalu ada, oleh karena itu pengelolaan risiko merupakan hal yang tepat untuk meminimalisasi potensi kerugian yang terjadi. Sehingga diperlukan IT Risk Management yang baik dalam suatu organisasi / perusahaan. IT Risk Management merupakan proses yang digunakan untuk mengurangi dan mengelola risiko yang mungkin terjadi dalam infrastruktur IT yang ada atau sistem yang diterapkan dalam organisasi. Manajemen risiko memegang peranan penting sebagai tindakan perlindungan asset sistem dan teknologi informasi.

2. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi!

   Jawab :

   Aspek *integrity* / integritas menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi, artinya informasi dijaga agar selalu akurat. Sebagai contoh, virus trojan merupakan contoh dari informasi yang integritasnya terganggu karena virus telah mengubah informasi tanpa izin. Kasus trojan horse merupakan distribusi paket program TCP Wrapper (yaitu program populer yang dapat digunakan untuk mengatur dan

membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak bertanggung jawab. Jika kita memasang program yang berisi trojan horse, maka ketika kita merakit (compile) program tersebut, email akan dikirim kepada orang tertentu yang kemudian memperbolehkan dia masuk ke sistem kita. Oleh karena itu, aspek integritas informasi ini dapat dijaga dengan melakukan enkripsi data atau dengan membuat tanda tangan digital (*digital signature*).

3. Pentingnya melakukan assessment terhadap insiden IT yang terjadi perlu dilakukan. Mengapa hal tersebut dalam manajemen risiko perlu dilaksanakan? Silakan berikan contoh (dan jika diperlukan kutipan dari sumber yang relevan).

   Jawab :

   Risk assessment atau penilaian risiko adalah kegiatan yang mempertimbangkan kemungkinan terjadinya suatu kejadian dan besar akibat yang bisa ditimbulkan oleh suatu kejadian. Berdasarkan hasil penilaian risiko maka dapat ditentukan peringkat risiko sehingga dapat dilakukakan pemilahan risiko dari yang besar sampai dengan risiko yang ringan sehingga dapat diabaikan. Hasil dari *risk assessment* (penilaian risiko) akan dijadikan dasar untuk melakukan *risk control*, yang kemudian *risk control* akan meminimalisir atau mengeliminasi risiko yang kemungkinan akan terjadi pada sebuah organisasi.

   Selain itu, dengan menggunakan penilaian risiko, sebuah organisasi dapat membuat keputusan yang lebih baik mengenai risiko dan mencapai tujuan bisnisnya. Menghilangkan ketidakpastian dengan menilai risiko memungkinkan sebuah organisasi mengelola operasinya dengan tingkat kepercayaan diri tertentu dan kegiatan atau proses dalam perusahaan bisa berjalan lebih efisien. Pemahaman ini mengantarkan pada sebuah keputusan apakah risiko yang telah teridentifikasi dapat diterima atau tidak, dan tindakan pengendalian apa yang paling tepat. Pada akhirnya, *output* dari penilaian risiko merupakan *input* terhadap proses pengambilan keputusan (ISO 31010 / ANSI Z690.3-2011).

   Referensi :

http://repository.its.ac.id/3110/1/5213100193-Undergraduate_Theses.pdf
http://journal.unair.ac.id/download-fullpapers-kklk0eec7060c92full.pdf
https://id.linkedin.com/pulse/risk-assessment-fundamental-fatih-dani-prasetio

4. DR atau Disaster Recovery merupakan bagian penting dari pengelolaan IT. Apa yang dimaksud dengan DR dan bagaimana DR dapat berkontribusi dalam mengurangi risiko terhadap penggunaan IT bagi organisasi?

   Jawab :

   Disaster (bencana) didefinisikan sebagai kejadian yang waktu terjadinya tidak dapat diprediksi dan bersifat sangat merusak. *Disaster Recovery* menurut terjemahan aslinya mengandung arti pemulihan bencana.

   Di dalam dunia IT, sangat penting untuk mengerti dan menerapkan Disaster Recovery Management. IT memegang peranan yang sangat penting saat terjadi bencana, karena di dalam sistem IT tersimpan informasi, data dan *core business* perusahaan yang mana di masa sekarang ini hampir semuanya sudah berjalan di atas sistem IT.

   Sebagai contoh, industri di sektor keuangan dan perbankan. Apabila suatu bank besar yang melayani jutaan nasabah dan mereka tidak memiliki IT Disaster Management yang baik. Suatu saat terjadi kebakaran pada *data center* (pusat data) pada bank tersebut, anggap saja dibutuhkan waktu 1 jam untuk memadamkan api tersebut dan dibutuhkan berhari–hari untuk memeriksa kerusakan serta perbaikan.

   Tidak dapat dibayangkan apabila data-data penting bagi perusahaan hilang karena suatu bencana (*disaster*), baik itu karena faktor alam maupun kesalahan manusia (*human error*). Sehingga merupakan suatu keharusan bagi sebuah organisasi untuk merencanakan suatu tindakan pengamanan terhadap arsip-arsip vital dalam rangka mengantisipasi bencana. Hal ini yang disebut dengan Disaster Recovery Planning.

5. Dalam lingkungan IT yang telah menerapkan Manajemen Risiko, penting melakukan peninjauan kembali terhadap standar yang telah ditetapkan. Mengapa hal tersebut perlu dan penting dilakukan?

   Jawab :

   Saat ini, lingkungan organisasi baik secara internal maupun eksternal menuntut pendekatan manajemen risiko yang terintegrasi dan tidak hanya fokus pada minimalisasi atau mitigasi risiko, tetapi juga mendukung kegiatan yang mendorong munculnya inovasi. Salah satu tahapan penyusunan standar manajemen risiko dalam sebuah organisasi yaitu pemantauan dan peninjauan ulang.

Pemantauan dan peninjauan ulang merupakan tahapan monitoring rutin terhadap kinerja aktual dari pelaksanaan proses manajemen risiko dibandingkan dengan rencana yang ditetapkan, yang kemudian dilakukan peninjauan berkala terhadap efektifitas sistem manajemen risiko yang diberlakukan dan efektifitas pelaksanaan penanganan risiko guna perbaikan secara kontinyu.

Proses manajemen risiko harus tetap dipantau dan ditinjau ulang untuk mengetahui adanya kendala dalam pelaksanaannya. Hal ini merupakan upaya untuk memastikan bahwa sistem manajemen risiko telah berjalan sesuai dengan rencana yang telah disepakati dan sejalan dengan ruang lingkup program.