PENGUKURAN RESIKO TEKNOLOGI INFORMASI DENGAN PENDEKATAN FRAP: STUDI KASUS PADA PT COWELL DEVELOPMENT, TBK

Iwan Kurniawan Widjaya

Computerized Accounting Department, School of Information Systems, Binus University
Jln. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
iwkkvk2011@yahoo.co.id; iwankw@binus.ac.id

ABSTRACT

The article purposes are to analyze, identify, and measure the risks found in the use of information technology. The research method used are literature study and field study upon observations, interviews, documentation, and FRAP (facilitated Risk Analysis Process) approach to measure the risk of information technology. The results found are positive and negative findings in the use of information technology. The exixting weaknesses allow the potential risks that may occur. The conclusion is there are vulnerabilities found in the use of information technology that need several recommendations on those risks to improve performance and guarantee data protection and information from any risk arise.

***Keywords**: risk, risk measurement, information technology, FRAP*

ABSTRAK

Tujuan artikel ini adalah menganalisis, mengidentifikasi, dan mengukur resiko-resiko resiko-resiko yang ditemukan atas penggunaan teknologi informasi. Metode penelitian yang digunakan adalah studi pustaka dan studi lapangan berupa observasi, wawancara, dan dokumentasi, serta pendekatan FRAP (Facilitated Risk Analysis Process) untuk mengukur resiko teknologi informasi. Hasil yang dicapai adalah temuan kelebihan dan kelemahan dalam penggunaan teknologi informasi. Kelemahan yang ada memungkinkan adanya potensi resiko yang dapat terjadi. Simpulan yang diperoleh adalah ditemukannya kerentanan dalam penggunaan teknologi informasi di perusahaan sehingga diperlukan rekomendasi terhadap resiko tersebut untuk meningkatkan kinerja, dan menjamin terlindungnya data dan informasi dari setiap resiko yang muncul.

***Kata kunci:** resiko, pengukuran resiko, teknologi informasi, FRAP*

PENDAHULUAN

Informasi teknologi, termasuk juga sistem informasi berbasis internet, saat ini merupakan suatu hal yang memainkan peranan vital dan sangat membantu dalam memperluas serta memajukan bisnis. Teknologi informasi dapat membantu segala jenis bisnis karena dapat meningkatkan efisiensi dan efektifitas proses bisnis, pengambilan keputusan manajerial, dan kolaborasi kelompok kerja (*workgroup*), sehingga hal tersebut dapat memperkuat posisi kompetitif bisnis perusahaan di pasar yang cepat sekali mengalami perubahan. Teknologi informasi ini juga digunakan untuk mendukung pengembangan produk, proses dukungan pelanggan, transaksi perdagangan elektronik (*e-commerce*), ataupun aktivitas bisnis lainnya. Teknologi informasi atau sistem informasi berbasis internet telah menjadi sebuah kebutuhan penting dalam kesuksesan di era perkembangan global saat ini (O'Brien & Marakas, 2007).

Jika teknologi informasi adalah hal yang akan memberikan dukungan tambahan bagi perusahaan maka resiko adalah hal yang bersifat kontraproduktif bagi perusahaan. Resiko merupakan ketidakpastian yang mungkin melahirkan peristiwa kerugian (Djojosoedarso, 2005).

Dengan adanya suatu manajemen resiko, resiko-resiko yang ada dapat dihilangkan, dikurangi, ataupun ditransfer. Oleh karena itu manajemen resiko di dalam suatu perusahaan amat penting dan dapat menghindari perusahaan dari kerugian-kerugian yang mungkin timbul di masa mendatang yang berasal dari resiko-resiko yang tidak dijadikan titik fokus di masa sekarang. (Gondodiyoto, 2009).

Tujuan penelitian adalah mengidentifikasi resiko-resiko yang ditemukan atas penggunaan teknologi informasi; melakukan pengukuran resiko terhadap teknologi informasi yang sudah diterapkan; mengetahui apakah di dalam perusahaan, penerapan teknologi informasi sudah memiliki peranan yang penting; mengidentifikasi praktek keamanan dan memberikan solusi yang terbaik untuk mengelola dan menanggulangi resiko. Manfaat penelitian ini yaitu memberikan informasi kepada perusahaan mengenai resiko yang ada pada teknologi informasi yang diterapkan; hasil penelitian dapat digunakan perusahaan untuk menyempunakan penerapan teknologi informasi perusahaan; memberikan alternatif solusi terhadap kelemahan atau resiko teknologi informasi perusahaan dan juga untuk mengurangi kerugian yang mungkin terjadi.

METODE

Pendekatan yang digunakan oleh penulis untuk melakukan resiko TI bersifat kualitatif. Metode yang dipakai berupa studi kasus pada PT Cowell Development, Tbk, antara lain:

Teknik Pengumpulan Data

Dalam penyusunan artikel ilmiah ini, data-data yang diperlukan diperoleh dari teknik pengumpulan data, sebagai berikut: (1) riset kepustakaan, yaitu dengan mengumpulkan data yang menggunakan sumber berupa buku atau bahan dari perpustakaan serta membaca literatur via *website* sebagai panduan dalam menyusun artikel ilmiah; (2) riset lapangan, yaitu dengan meninjau langsung ke PT Cowell Development, Tbk dengan tujuan untuk memperoleh data yang dibutuhkan untuk penelitian. Adapun caranya sebagai berikut: (a) wawancara (*interview*), dengan cara tanya jawab secara langsung melalui pihak yang berkepentingan dalam perusahaan sehingga didapatkan data yang tepat dan berkualitas; (b) pengamatan (observasi), dengan meninjau secara langsung terhadap objek yang akan diteliti penulis disini berkaitan dengan kondisi TI yang dipakai perusahaan yang mencakup *hardware*, *software*, jaringan, aplikasi, dan prosedur yang diterapkan perusahaan.

Teknik Analisis

Ada berbagai metode dan pendekatan dalam menganalisis resiko salah satunya adalah FRAP (*Facilitated Risk Analysis Process*) (Peltier, 2001). FRAP merupakan suatu pendekatan dalam melakukan analisis resiko kualitatif. FRAP dikembangkan sebagai proses yang efisien dan disiplin untuk menjamin resiko informasi terkait keamanan yang berhubungan dengan operasi bisnis dipertimbangkan dan didokumentasikan. Dengan menggunakan FRAP diharapkan proses analisis resiko dapat dilakukan dalam hitungan hari, bukan mingguan atau bulanan. Dengan demikian analisis resiko bukan merupakan kendala, tetapi proses yang sangat mungkin dilakukan dan juga diperlukan. FRAP bukan suatu metodologi, tetapi suatu pendekatan terhadap proses penentuan resiko dan dampaknya, proses penentuan prioritas, dan proses penentuan kontrol pengamanan. Pendekatan FRAP (*Facilitated Risk Analysis Process*) adalah bentuk pendekatan analisis resiko kualitatif yang paling banyak digunakan saat ini. Dari teknik yang ada untuk mengukur resiko teknologi informasi, penulis memutuskan untuk menggunakan pendekatan FRAP.

FRAP (Peltier, 2001) dikembangkan sebagai proses yang efisien dan disiplin untuk menjamin resiko informasi terkait keamanan yang berhubungan dengan operasi bisnis dipertimbangkan dan didokumentasikan. Prosesnya melibatkan penganalisisan satu sistem, aplikasi, atau segmen dari operasi bisnis pada satu waktu dan mengumpulkan sebuah tim dari individu-individu termasuk manajer bisnis yang akrab dengan kebutuhan informasi bisnis dan staf teknis yang memiliki pemahaman yang rinci tentang kelemahan sistem yang potensial dan terkait kontrol.

Selama sesi FRAP, tim mengungkapkan pendapat tentang ancaman yang potensial, *vulnerability*, dan hasil dari dampak negatif pada *integrity* data, *confidentiality*, serta *availability*. Lalu tim akan menganalisis pengaruh dampak tersebut terhadap operasi bisnis dan secara luas mengkategorikan resiko menurut prioritas levelnya. Tim biasanya tidak mencoba untuk mendapatkan atau mengembangkan angka yang spesifik untuk kemungkinan terjadinya ancaman atau perkiraan kerugian tahunan meskipun data untuk menentukan faktor-faktor tersebut tersedia. Tim bergantung pada pengetahuan umum dari ancaman dan kerentanan yang diperoleh dari pusat respon insiden nasional, asosiasi profesi dan literatur, dan pengalaman mereka sendiri.

Setelah mengidentifikasi dan mengkategorikan resiko, tim mengidentifikasi pengendalian-pengendalian yang dapat diimplementasikan untuk mengurangi resiko, berfokus pada pengendalian yang paling efektif dari segi biaya. Tim akan menggunakan titik awal dari 26 kontrol umum yang dirancang untuk mengatasi berbagai jenis resiko. Pada akhirnya, keputusan seperti apa yang dibutuhkan terkait pengendalian terletak pada manajer bisnis yang mempertimbangkan sifat aset-aset informasi dan pentingnya mereka bagi operasi bisnis dan biaya pengendalian.

Kesimpulan tim mengenai resiko-resiko apa yang ada, bagaimana prioritasnya, dan pengendalian apa yang yang dibutuhkan, didokumentasikan dan dikirim kepada pimpinan proyek dan manajer bisnis untuk menyelesaikan rencana aksi.

Tiap proses analisis resiko (Peltier, 2001) dibagi menjadi tiga sesi yang berbeda: *pre-FRAP meeting*, *FRAP session*, dan *post-FRAP session*.

Pre-FRAP Meeting

Pre-FRAP *meeting* ini merupakan kunci sukses dalam suatu proyek. Pada tahap ini pertemuan biasanya berlangsung sekitar satu jam dan biasanya dilakukan di kantor klien.

Ada 5 komponen utama yang muncul dari sesi ini: (1) *scope statement* – pimpinan proyek dan manajer bisnis harus menentukan ruang lingkup pembahasan; (2) *visual model* – pembuatan diagram

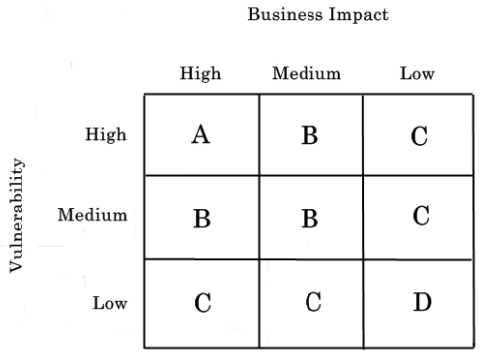
proses (gambaran) mengenai pernyataan ruang lingkup untuk ditinjau kembali; (3) *team members* – membangun tim FRAP yang terdiri atas tujuh hingga 15 orang anggota yang berhubungan dengan sistem yang terkait; (3) *meeting mechanics* – manager bisnis bertanggung jawab dalam menyediakan ruangan *meeting,* menyusun jadwal, dan juga menyiapkan bahan-bahan yang dibutuhkan; (4) *agreement of definition* – dalam sesi pre-FRAP dibutuhkan persetujuan terhadap definisi FRAP. Persetujuan tersebut haruslah berdasarkan pada adanya *risk, control, impact,* dan *vulnerability*. Selama sesi pre-FRAP sangatlah penting untuk mendiskusikan ancaman utama dalam proses bisnis.

FRAP Session

Pada tahap ini pertemuan biasanya berlangsung selama empat jam. Komponen-komponen yang muncul dari tahap ini di antaranya adalah: (1) *identified risks* – mengidenifikasi resiko yang mungkin terjadi pada sistem bisnis perusahaan; (2) *priotized risks* – menentukan resiko utama dari semua resiko yang mungkin terjadi (yang memilki ancaman terbesar); (3) *suggested controls* – memberikan solusi pengendalian untuk meminimalisir resiko dan juga ancaman yang mungkin terjadi.

Definisi-definisi dalam tahap ini yang harus dipahami sebagai berikut: *High vulnerability*: tingkat kelemahan yang sangat besar yang ada di dalam sistem atau operasional perusahaan, dimana dampak potensi terhadap bisnis sangatlah besar dan signifikan , sehingga kontrolnya harus ditingkatkan.
Medium vulnerability: terdapatnya beberapa kelemahan yang muncul, dan ketika dampak potensi terhadap bisnis mulai muncul dengan tingkat yang besar atau signifikan, maka kontrolnya dapat lebih ditingkatkan.

Low vulnerability: sistem yang ada sudah dioperasikan dengan baik dan benar. Tidak dibutuhkannya kontrol untuk mengurangi kerentanan. *Severe impact (high)*: dapat menjatuhkan usaha dari bisnis yang ada atau memberikan kerusakan yang parah terhadap prospek dan perkembangan perusahaan. *Significant impact (medium)*: dapat mengakibatkan kerusakan dan kerugian biaya yang signifikan, tetapi usaha/ bisnis tetap akan bertahan. *Minor impact (low)*: tipe dampak yang cukup operasional terhadap bisnis, dimana dampak ini tetap dikelola sebagai bagian dari rutinitas bisnis biasa. Berikut merupakan Matrix Prioritas dalam menganalisis aksi dan kontrol yang harus diimplementasikan berdasarkan tipe tinggi atau rendahnya dampak bisnis dan tingkat kerentanan yang dapat terjadi pada sistem perusahaan.



Gambar 1. Priority risk matrix.

A : Tindakan korektif harus diimplementasikan
B : Tindakan korektif sebaiknya diimplementasikan
C : Dibutuhkan *monitoring* (pengawasan)
D : Tidak ada tindakan yang diperlukan

Post-FRAP Meeting

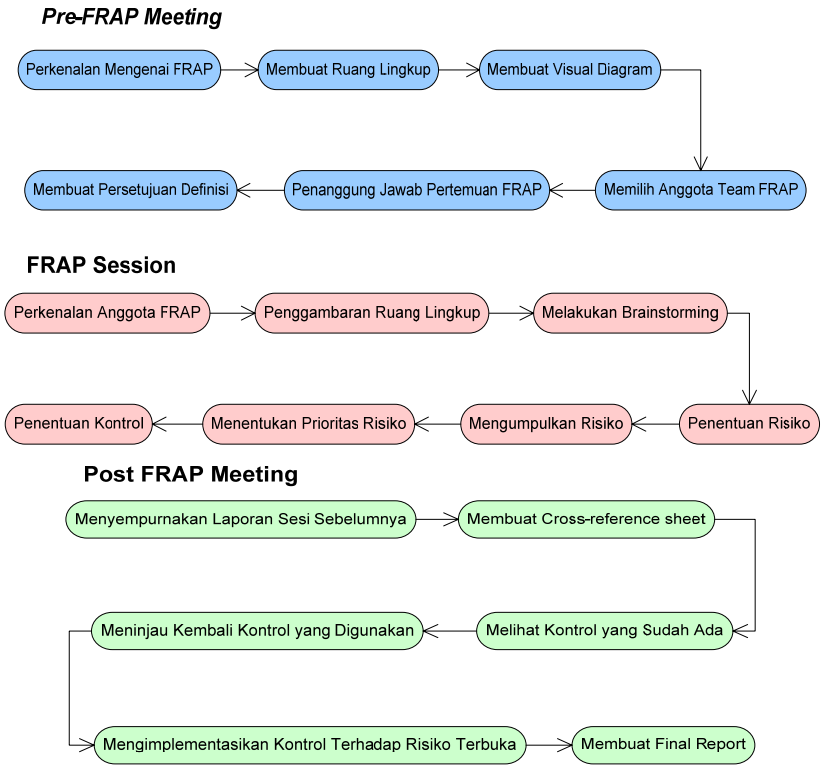
Pada tahap ini pertemuan biasanya berlangsung selama empat jam dan memiliki tiga elemen: (1) *creation on the cross-reference sheet* – membuat *cross-reference sheet* yang berisikan masing-masing kontrol dan resiko-resiko apa saja yang dapat berkurang sebagai akibat dari pelaksanaan kontrol tersebut; (2) *identification of existing controls* – meninjau ulang, mengidentifikasi kontrol apa saja yang dapat digunakan untuk mengatasi resiko-resiko yang masih terbuka; (3) *selection of controls for open risks or acceptance of risk* - menentukan *control* apa saja yang perlu dilakukan untuk menganggulangi resiko yang masih ada. Atau bahwa ternyata resiko tersebut tidaklah bersifat *high impact* sehingga bisnis manajer mengindikasikan resiko tersebut sebagai resiko yang dapat diterima.

HASIL DAN PEMBAHASAN

Pre-FRAP Meeting

Ruang Lingkup

Dalam pernyataan ruang lingkup ini kami sebagai fasilitator FRAP menentukan ruang lingkup mana saja yang akan diambil, dalam hal ini diambil ruang lingkup di bidang TI (Sistem informasi dan infrastruktur) dalam PT Cowell Development, Tbk. Akan tetapi bukan berarti tidak ada bagian lain yang terkait; ada keterkaitan secara tidak langsung seperti kepada Bagian Marketing dan Keuangan. Gambaran Proses FRAP (Gambar 2).



Gambar 2. Gambaran (visual model) proses FRAP.

Menentukan Anggota FRAP

Selama proses *FRAP Meeting* ini Fasilitator FRAP perlu menentukan siapa saja yang terkait dalam *FRAP Team*, hal ini dapat membantu fasilitator dalam melakukan *brainstorming* terhadap resiko yang mungkin muncul, resiko yang telah muncul maupun kontrol yang telah ada. Adapun anggota yang melakukan *brainstorming* ini yaitu: General Manager TI, Kepala dari Sistem Informasi terkait, Kepala Infrakstruktur dan Jaringan, Staff TI, Manajer Bisnis, Pimpinan Proyek, Fasilitator, dan Juru tulis.

Pertemuan Teknis

Dalam proses *Meeting Mechanics* ini manajer bisnis memilih seseorang dari stafnya untuk bertanggung jawab terhadap ketersediaan ruang *meeting*, menentukan jadwal *meeting* serta menyiapkan kebutuhan yang diperlukan untuk jalannya *meeting*.

Persetujuan Definisi

Dalam tahap ini fasilitator perlu menentukan persetujuan terhadap definisi terhadap elemen-elemen yang muncul pada resiko yaitu: (1) *integrity* – segala macam informasi tanpa adanya modifikasi yang tidak sah (asli); (2) *confidentiality* – informasi yang ada diperusahaan bersifat rahasia dan hanya pihak yang berwenang yang dapat mengakses dari informasi tersebut; (3) a*vailability* – aplikasi, sistem, atau sumber informasi yang diperlukan oleh perusahaan tersedia saat dibutuhkan. Hendaknya seluruh anggota FRAP dapat mengerti dan memahami dengan pasti dari ketiga elemen tersebut.

FRAP Session

Berikut beberapa hal yang ditemukan mengenai identifikasi resiko (Tabel 1), kontrol terhadap resiko (Tabel 2), dan prioritasi resiko (Tabel 3).

Tabel 1
Identifikasi Resiko

No.	Resiko
1	Informasi diakses oleh pihak yang tidak berwenang
2	Kurangnya proses *internal* untuk membuat dan mengendalikan, mengelola data di seluruh fungsi
3	Informasi digunakan dalam konteks yang tidak sesuai
4	Data diperbarui secara *internal* tapi tidak dibuat eksternal
5	Informasi pihak ketiga dapat menyebabkan masalah kepada perusahaan
6	Otorisasi keaslian permintaan data
7	Penolakan akses ke informasi padahal diakses oleh orang yang berwenang
8	Penggunaan informasi yang tidak benar yang dapat berdampak pada bisnis
9	Prosedur otorisasi pada perusahaan
10	Proses kontrol yang terlalu rumit
11	Kurangnya personil dibidang sistem aplikasi
12	Informasi dikeluarkan tanpa otorisasi yang tepat
13	Kebocoran informasi *internal* perusahaan
14	Tidak menanggapi permintaan secara tepat waktu

15	Personil *internal* sengaja memodifikasi data untuk pribadi/keuntungan kelompok
16	Tidak adanya kepercayaan bisnis dengan mitra pihak ketiga
17	Tidak adanya rekaman terhadap perubahan sistem/aplikasi *software*
18	Data lama/dokumen tidak dihapus
19	Modifikasi anti virus terhadap perkembangan virus
20	Kesalahan terhadap data/ dokumen yang dipublikasikan
21	Informasi dari mitra atau pemasok terjadi kesalahan
22	Informasi/ data tidak benar
23	Salah pengelompokan informasi/data
24	Akses terhadap pelanggan/mitra kerja tidak tersedia secara lengkap
25	Mantan *user*/ karyawan masih memiliki akses untuk mengamankan data
26	Menggunakan sistem yang rentan untuk mengirim data/ informasi yang penting
27	Akses yang tidak terkendali terhadap informasi yang rahasia
28	Informasi sensitif dan tidak sensitif menjadi satu
29	Otentikasi untuk akses informasi sensitif tidak memadai
30	Penyalahgunaan *user id*
31	Akses untuk *backup* data tidak terkontrol dengan baik
32	Keamanan *firewall* diintrusi
33	Pihak ketiga membatalkan perjanjian yang telah dibuat
34	*Hacker* dapat membuat sistem *down*
35	Situs *hosting* tidak memiliki perlindungan fisik informasi
36	Hubungan jaringan antar sistem gagal didalam perusahaan
37	Desain sistem terlalu rumit
38	Kesalahan terhadap instalasi *software*/*hardware*
39	Kebutuhan *backup* tidak memadai
40	Kesalahan konfigurasi *hardware*
41	Kurangnya pelatihan bagi *user*
42	Terdapatanya virus dapat menyebabkan kegagalan sistem/ hilangnya data
43	*Router* yang tidak berfungsi dengan baik dapat menyebabkan sulitnya akses pada layanan
44	Ketidaktersediaan dokumen DRP dalam perusahaan
45	Tidak adanya *Emergency Respon Procedure* yang diimplementasikan di perusahaan

Tabel 2
Kontrol terhadap Resiko

No.	Kontrol	Deskripsi Kontrol
1	*Clear visualization*	Terdapat suatu proses bisnis yang lengkap sehingga memungkinkan bagi perusahaan melihat gambaran secara jelas proses bisnis yang akan dijalankan.
2	*Information authorization*	Penggunaan informasi dalam perusahaan dipakai dengan cara yang tepat karena setiap tindakan yang dilakukan berdasarkan arahan dari yang berwenang dan tanpa adanya pemalsuan informasi (otorisasi yang tepat)
3	*Internal update*	Data dalam perusahaan (*internal*) selalu diperbarui secara berkala.

4	*Confidential access*	Adanya sistem keamanan dalam sistem informasi sehingga tidak sembarang orang dapat mengakses langsung dalam sistem (khususnya orang dari pihak luar).
5	*Access authorization*	Setiap akses yang diberikan kepada karyawan perusahaan melalui ijin dari atasan, dan selalu dikonfirmasi dengan baik kepada pengguna.
6	*Modify authorization*	Dalam mengupdate/memodifikasi data diperlukan surat perintah dari atasan, tidak boleh sembarang merubah, menambah, ataupun menghilangkan data.
7	*Data classification*	Setiap data memiliki pengelompokannya masing-masing, dan secara teratur dikordinasi oleh pihak TI.
8	*Third party communication clearly*	Adanya komunikasi yang jelas dengan mitra kerja/pihak ketiga.
9	*Remove access*	Setiap pengguna yang telah keluar perusahaan (*resign*), akan langsung dicabut aksesnya terhadap akses sistem informasi.
10	*Adequately network*	Sistem penyaluran informasi/akses dalam perusahaan memiliki kualitas yang baik dan terjaga kerahasiaannya.
11	*Virus protected*	Setiap Laptop dan *Personal Computer* harus memiliki perlindungan *Firewall* dan Antivirus yang sesuai standar perusahaan.
12	*Id requirment*	Setiap pengguna memiliki satu ID *user*.
13	*Disaster recovery planning*	Rencana pemulihan dari kemungkinan kerusakan-kerusakan yang berdampak pada kemampuan proses komputer dan operasi bisnis perusahaan.
14	*Good server quality*	Perusahaan memiliki *server* yang baik dan memadai.
15	*Good of Bussiness Partner*	Perusahaan memiliki mitra bisnis yang baik dan memadai.
16	*Update of Operating System*	Perusahaan mengikuti perkembangan zaman terhadap OS (*operating system*) komputer.
17	*Backup*	Persyaratan cadangan akan ditentukan dan dikomunikasikan ke penyedia layanan, termasuk permintaan bahwa pemberitahuan elektronik di mana cadangan diselesaikan, dikirim ke administrator sistem aplikasi. Operasional akan diminta untuk menguji prosedur cadangan.
18	*Recovery plan*	Mengembangkan, mendokumentasikan, dan menguji prosedur pemulihan yang dirancang untuk merancang untuk memastikan bahwa aplikasi dan informasi dapat diperoleh kembali, dengan menggunakan cadangan yang dibuat, jika terjadinya kemungkinan kehilangan data.
19	*Access control*	Menerapkan mekanisme kontrol akses untuk mencegah akses yang tidak sah terhadap informasi. Mekanisme ini akan mencakup kemampuan untuk mendeteksi, dan melaporkan pencobaan terhadap keamanan informasi.
20	*Access control*	Sumber akses adalah menerapkan mekanisme untuk membatasi akses ke informasi rahasia dan ke jalur jaringan tertentu atau lokasi fisik.
21	*Access control*	Melaksanakan mekanisme otentikasi pengguna (seperti *firewall*, tombol/*dial-in* kontrol, keamanan ID) untuk membatasi akses ke petugas yang berwenang.
22	*Access control*	Melaksanakan mekanisme enkripsi data untuk mencegah akses yang tidak sah untuk melindungi integritas sebuah kerahasiaan informasi.
23	*Application control*	Merancang dan menerapkan pengendalian aplkasi (pengecekan pemasukan data lapangan yang memerlukan validasi, indikator alarm, kemampuan sandi kadaluarsa, pengecekan jumlah) untuk menjamin integritas, kerahasiaan, dan ketersediaan informasi aplikasi.

24	*Acceptance testing*	Mengembangkan prosedur pengujian yang harus diikuti selama aplikasi dan selama modifikasi aplikasi yang sudah ada yang mencakup penggunaan partisipasi dan penerimaan.
25	*Change management*	Mematuhi suatu proses perubahan manajemen yang dirancang untuk memfasilitasikan pendekatan struktur untuk modifikasi, untuk memastikan langkah yang tepat dan tindakan pencegahan akan dipatuhi. Modifikasi yang dilakukan secara mendesak harus dimasukan dalam proses ini.
26	*Anti-virus*	Memastikan administrator LAN menginstal anti-virus perangkat lunak standar perusahaan di semua komputer. Serta adanya pelatihan dan kesadaran teknik pencegahan virus yang digabungkan dalam program organisasi.
27	*Policy*	Mengembangkan kebijakan dan prosedur untuk membatasi akses dan mengoperasikan hak istimewa bagi mereka yang membutuhkan bisnis.
28	*Training*	Pengguna pelatihan akan mencakup instruksi dan dokumentasi tentang penggunaan aplikasi secara benar. Pentingnya menjaga kerahasiaan dari account pengguna/rekening pemakai, sandi, dan sifat rahasia dan kompetitif informasi akan ditekankan.
29	*Audit/monitor*	Melaksanakan mekanisme untuk memantau/ mengawasi, melaporkan, dan kegiatan audit yang diidentifikasi sebagai yang memerlukan tinjauan independen, termasuk tinjauan berkala *user ID* untuk memastikan dan memverifikasi kebutuhan bisnis.
30	*Backup*	Kontrol operasi adalah pelatihan untuk cadangan ke sistem administrator akan disediakan dan tugas diputar diantara mereka untuk memastikan kecukupan/ kemampuan dari program pelatihan.
31	*Training*	Operasi pengendalian: pengembangan aplikasi akan memberikan dokumentasi, bimbingan, dan dukungan untuk staff operasi dalam melaksanakan mekanisme untuk memastikan bahwa transfer informasi antara aplikasi aman.
32	*Access control*	Operasi kontrol: mekanisme untuk melindungi terhadap resiko database yang tidak sah, dan modifikasi yang dilakukan dari luar aplikasi, akan ditentukan dan diimplementasikan.
33	*Interface dependencies*	Operasi kontrol: sistem yang memberikan informasi akan diidentifikasi dan dikomunikasikan ke penyedia layanan untuk menekankan dampak terhadap fungsi jika bagian aplikasi ti tidak berada di tempat.
34	*Maintenance*	Operasi kontrol: waktu persayaratan untuk pemeliharaan teknis akan dilacak dan permintaan untuk penyesuaian akan dikomunikasikan kepada manajemen.
35	*Training*	Kontrol Pengguna: melaksanakan program pengguna (pengguna evaluasi kinerja) yang dirancang untuk mendorong kepatuhan terhadap kebijakan dan prosedur untuk memastikan penggunaan aplikasi yang tepat.
36	*Service level agreement*	Perjanjian tingkat memperoleh layanan adalah untuk menetapkan tingkat harapan pelanggan dan jaminan dari mendukung operasi.
37	*Maintenance*	Memperoleh pemeliharaan atau perjanjian penyaluran/ penyedia untuk memfasilitasi berkelanjutan status operasional aplikasi.
38	*Physical security*	Dalam konsultasi dengan manajemen fasilitas, memfasilitasi pelaksanaan kontrol keamanan fisik yang dirancang untuk melindungi informasi, perangkat lunak dan perangkat keras yang membutuhkan sistem.
39	*Management support*	Permintaan dukungan manajemen untuk menjamin kerjasama dan koordinasii berbagai unit bisnis, untuk memfasilitasi kelancaran transisi ke aplikasi.
40	*Proprietary*	Kepemilikan kontrol.
41	*Corrective strategies*	Tim pengembang akan mengembangkan strategi korektif seperti proses ulang, merevisi/ merubah logika aplikasi, dll.

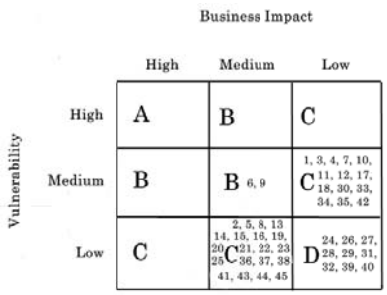
42	*Change management*	Produksi kontrol migrasi seperti pencarian dan menghapus/ menghilangkan proses untuk memastikan penyimpanan data yang bersih.
43	*Monitoring*	Melakukan pemerikasaan secara rutin (berkala) terhadap *hardware, software*, dan sistem informasi yang ada.

Tabel 3
Prioritasi Resiko

No.	Resiko	Tipe	Prioritas	Kontrol
1	Informasi diakses oleh pihak yang tidak berwenang	INT	C	18, 20, 21, 27, 40
2	Kurangnya proses *internal* untuk membuat dan mengendalikan, mengelola data di seluruh fungsi	INT	C	29, 32, 36
3	Informasi digunakan dalam konteks yang tidak sesuai	INT	C	1, 2, 40
4	Data diperbarui secara *internal* tapi tidak dibuat eksternal	INT	C	3, 25, 43
5	Informasi pihak ketiga dapat menyebabkan masalah kepada perusahaan	INT	C	4, 25, 27
6	Otorisasi keaslian permintaan data	INT	B	21, 22, 26
7	Penolakan akses ke informasi padahal diakses oleh orang yang berwenang	INT	C	5, 18, 25, 27
8	Penggunaan informasi yang tidak benar yang dapat berdampak pada bisnis	INT	C	17, 24, 27, 28, 30, 31, 41
9	Prosedur otorisasi pada perusahaan	INT	B	18, 21, 34, 38, 40, 43
10	Proses kontrol yang terlalu rumit	INT	C	31, 35
11	Kurangnya personil dibidang sistem aplikasi	INT	C	26, 27, 28, 34
12	Informasi dikeluarkan tanpa otorisasi yang tepat	INT	C	26, 27, 28, 34, 39, 43
13	Kebocoran informasi *internal* perusahaan	INT	C	2, 4 ,19, 20 ,21, 38, 43
14	Tidak menanggapi permintaan secara tepat waktu	INT	C	28, 34, 36
15	Personil *internal* sengaja memodifikasi data untuk pribadi/keuntungan kelompok	INT	C	2, 6, 25
16	Tidak adanya kepercayaan bisnis dengan mitra pihak ketiga	INT	C	27, 36, 38
17	Tidak adanya rekaman terhadap perubahan sistem/aplikasi *software*	INT	C	18, 25, 43
18	Data lama/dokumen tidak dihapus	INT	C	24, 41, 43
19	Modifikasi anti virus terhadap perkembangan virus	INT	C	17, 25, 26, 27, 28, 43
20	Kesalahan terhadap data/ dokumen yang dipublikasikan	INT	C	22, 23, 24, 41
21	Informasi dari mitra atau pemasok terjadi kesalahan	INT	C	22, 27, 28, 32, 37
22	Informasi/ data tidak benar	CON	C	26, 27, 28, 43
23	Salah pengelompokan informasi/data	CON	C	7, 25

24	Akses terhadap pelanggan/mitra kerja tidak tersedia secara lengkap	CON	D	8, 25
25	Mantan *user*/ karyawan masih memiliki akses untuk mengamankan data	CON	C	9, 25
26	Menggunakan sistem yang rentan untuk mengirim data/ informasi yang penting	CON	D	10, 25, 43
27	Akses yang tidak terkendali terhadap informasi yang rahasia	CON	D	19, 21, 22, 37
28	Informasi sensitif dan tidak sensitif menjadi satu	CON	D	22, 23, 26, 27, 30
29	Otentikasi untuk akses informasi sensitif tidak memadai	CON	D	10, 34, 38, 43
30	Penyalahgunaan *user id*	CON	C	12, 25
31	Akses untuk *backup* data tidak terkontrol dengan baik	CON	D	13, 25, 42, 43
32	Keamanan *firewall* diintrusi	CON	D	17, 18, 38, 43
33	Pihak ketiga membatalkan perjanjian yang telah dibuat	CON	C	8, 20, 27
34	*Hacker* dapat membuat sistem *down*	AVA	C	16, 17, 18 ,20, 21, 25, 36, 37, 43
35	Situs *hosting* tidak memiliki perlindungan fisik informasi	AVA	C	11, 35, 37, 43
36	Hubungan jaringan antar sistem gagal didalam perusahaan	AVA	C	14, 15, 17, 43
37	Desain sistem terlalu rumit	AVA	C	28, 31, 33
38	Kesalahan terhadap instalasi *software*/*hardware*	AVA	C	23, 24, 43
39	Kebutuhan *backup* tidak memadai	AVA	D	13, 34
40	Kesalahan konfigurasi *hardware*	AVA	D	16, 17, 18, 34
41	Kurangnya pelatihan bagi *user*	AVA	C	27, 30
42	Terdapatanya virus dapat menyebabkan kegagalan sistem/ hilangnya data	AVA	C	16, 17, 25
43	*Router* yang tidak berfungsi dengan baik dapat menyebabkan sulitnya akses pada layanan	AVA	C	33, 35, 37
44	Ketidaktersediaan dokumen DRP dalam perusahaan	AVA	C	13, 18, 19
45	Tidak adanya *Emergency Respon Procedure* yang diimplementasikan di perusahaan	AVA	C	8, 17, 18

Gambar 3 berikut ini merupakan *priority risk matrix.*



Gambar 3. Priority risk matrix: penyebaran *suggested risks.*

Post-FRAP Meeting

Control/Risks Cross-Reference List

Control/Risks Cross-reference List bertujuan untuk menentukan control mana yang dapat memitigasi resiko-resiko. Dalam *Control/Risks Cross-reference List* (Tabel 4) ini kita dapat melihat satu control dapat memitigasi lebih dari satu resiko sehingga dapat membantu dalam menentukan sumber daya mana yang paling baik untuk menangani resiko tersebut. Pimpinan proyek dan fasilitator akan melihat kontrol mana saja yang sudah berada tepat di tempatnya (resiko). Kemudian tim membuat rencana aksi yang berisikan kontrol mana yang akan dilaksanakan, berikut disertai dengan tanggal pelaksanaan atau implementasi kontrol beserta dengan pihak mana yang akan melakukan implementasi kontrol tersebut.

Tabel 4
Control/Risks Cross-Reference List

No.	Deskripsi Kontrol	Resiko	Deskripsi Resiko	Tipe	Prioritas
1	Terdapat suatu proses bisnis yang lengkap sehingga memungkinkan bagi perusahaan melihat gambaran secara jelas proses bisnis yang akan dijalankan.	3	Informasi digunakan dalam konteks yang tidak sesuai	INT	C
2	Penggunaan informasi dalam perusahaan dipakai dengan cara yang tepat karena setiap tindakan yang dilakukan berdasarkan arahan dari yang berwenang dan tanpa adanya pemalsuan informasi (otorisasi yang tepat)	3	Informasi digunakan dalam konteks yang tidak sesuai	INT	C
		13	Kebocoran informasi internal perusahaan	INT	C
		15	Personil *internal* sengaja memodifikasi data untuk pribadi/keuntungan kelompok	INT	C
3	Data dalam perusahaan (internal) selalu di perbarui secara berkala.	4	Data diperbarui secara *internal* tapi tidak dibuat eksternal	INT	C
4	Adanya sistem keamanan dalam sistem informasi sehingga tidak sembarang orang dapat mengakses langsung dalam sistem (khususnya orang dari pihak luar).	5	Informasi pihak ketiga dapat menyebabkan masalah kepada perusahaan	INT	C
		13	Kebocoran informasi internal perusahaan	INT	C
5	Setiap akses yang diberikan kepada karyawan perusahaan melalui ijin dari atasan, dan selalu dikonfirmasi dengan baik kepada pengguna.	7	Penolakan akses ke informasi padahal diakses oleh orang yang berwenang	INT	C
6	Dalam mengupdate/memodifikasi data diperlukan surat perintah dari atasan, tidak boleh sembarang merubah, menambah, ataupun menghilangkan data.	15	Personil *internal* sengaja memodifikasi data untuk pribadi/keuntungan kelompok	INT	C

7	Setiap data memiliki pengelompokannya masing-masing, dan secara teratur dikordinasi oleh pihak TI.	23	Salah pengelompokan informasi/data	CON	C
8	Adanya komunikasi yang jelas dengan mitra kerja/pihak ketiga.	24	Akses terhadap pelanggan/mitra kerja tidak tersedia secara lengkap	CON	D
		33	Pihak ketiga membatalkan perjanjian yang telah dibuat	CON	C
		45	Tidak adanya Emergency Respon Prosedur yang diimplementasikan di perusahaan	AVA	C
9	Setiap pengguna yang telah keluar perusahaan (resign), akan langsung dicabut aksesnya terhadap akses sistem informasi.	25	Mantan *user*/ karyawan masih memiliki akses untuk mengamankan data	CON	C
10	Sistem penyaluran informasi/akses dalam perusahaan memiliki kualitas yang baik dan terjaga kerahasiaannya.	26	Menggunakan sistem yang rentan untuk mengirim data/ informasi yang penting	CON	D
		29	Otentikasi untuk akses informasi sensitif tidak memadai	CON	D
11	Setiap Laptop dan Personal Komputer harus memiliki perlindungan Firewall dan Antivirus yang sesuai standar perusahaan.	35	Situs *hosting* tidak memiliki perlindungan fisik informasi	AVA	C
12	Setiap pengguna memiliki satu ID *user*.	30	Penyalahgunaan *user* ID	CON	C
13	Rencana pemulihan dari kemungkinan kerusakan-kerusakan yang berdampak pada kemampuan proses komputer dan operasi bisnis perusahaan.	31	Akses untuk *backup* data tidak terkontrol dengan baik	CON	D
		39	Kebutuhan *backup* tidak memadai	AVA	D
		44	Ketidaktersediaan dokumen DRP dalam perusahaan	AVA	C
14	Perusahaan memiliki *server* yang baik dan memadai.	36	Hubungan jaringan antar sistem gagal didalam perusahaan	AVA	C
15	Perusahaan memiliki mitra bisnis yang baik dan memadai.	36	Hubungan jaringan antar sistem gagal didalam perusahaan	AVA	C
16	Perusahaan mengikuti perkembangan zaman terhadap OS komputer.	34	*Hacker* dapat membuat sistem *down*	AVA	C
		40	Konfigurasi *hardware* yang tidak memadai	AVA	D
		42	Terdapatanya virus dapat menyebabkan kegagalan sistem/hilangnya data	AVA	C

17	Persyaratan cadangan akan ditentukan dan dikomunikasikan ke penyedia layanan, termasuk permintaan bahwa pemberitahuan elektronik dimana cadangan diselesaikan, dikirim ke administrator sistem aplikasi. Operasional akan diminta untuk menguji prosedur cadangan.	8	Penggunaan informasi yang tidak benar yang dapat berdampak pada bisnis	INT	C
		19	Modifikasi anti virus terhadap perkembangan virus	INT	C
		32	Keamanan *firewall* diintrusi	CON	D
		34	*Hacker* dapat membuat sistem *down*	AVA	C
		36	Hubungan jaringan antar sistem gagal didalam perusahaan	AVA	C
		40	Kesalahan konfigurasi *hardware*	AVA	C
		42	Terdapatanya virus dapat menyebabkan kegagalan sistem/ hilangnya data	AVA	C
		45	Tidak adanya *Emergency Respon Procedure* yang diimplementasikan di perusahaan	AVA	C
18	Mengembangkan, mendokumentasikan, dan menguji prosedur pemulihan yang dirancang untuk merancang untuk memastikan bahwa aplikasi dan informasi dapat diperoleh kembali, dengan menggunakan cadangan yang dibuat, jika terjadinya kemungkinan kehilangan data.	1	Informasi diakses oleh pihak yang tidak berwenang	INT	C
		7	Penolakan akses ke informasi padahal diakses oleh orang yang berwenang	INT	C
		9	Prosedur otorisasi pada perusahaan	INT	B
		17	Tidak adanya rekaman terhadap perubahan sistem/aplikasi *software*	INT	C
		32	Keamanan *firewall* diintrusi	CON	D
		34	*Hacker* dapat membuat sistem *down*	AVA	C
		40	Konfigurasi *hardware* yang tidak memadai	AVA	D
		44	Ketidaktersediaan dokumen DRP dalam perusahaan	AVA	C
		45	Tidak adanya Emergency Response Procedure yang diimplementasikan di perusahaan	AVA	C

19	Menerapkan mekanisme kontrol akses untuk mencegah akses yang tidak sah terhadap informasi. Mekanisme ini akan mencakup kemampuan untuk mendeteksi, dan melaporkan pencobaan terhadap keamanan informasi.	13	Kebocoran informasi internal perusahaan	INT	C
		27	Akses yang tidak terkendali terhadap informasi yang rahasia	CON	D
		44	Ketidaktersediaan dokumen DRP dalam perusahaan	AVA	C
20	Sumber akses adalah menerapkan mekanisme untuk membatasi akses ke informasi rahasia dan ke jalur jaringan tertentu atau lokasi fisik.	1	Informasi diakses oleh pihak yang tidak berwenang	INT	C
		13	Kebocoran informasi internal perusahaan	INT	C
		33	Pihak ketiga membatalkan perjanjian yang telah dibuat	CON	C
		34	*Hacker* dapat membuat sistem *down*	AVA	C
21	Melaksanakan mekanisme otentikasi pengguna (seperti firewall, tombol/dial-in kontrol, keamanan ID) untuk membatasi akses ke petugas yang berwenang.	1	Informasi diakses oleh pihak yang tidak berwenang	INT	C
		6	Otorisasi keaslian permintaan data	INT	B
		9	Prosedur otorisasi pada perusahaan	INT	B
		13	Kebocoran informasi internal perusahaan	INT	C
		27	Akses yang tidak terkendali terhadap informasi yang rahasia	CON	D
		34	*Hacker* dapat membuat sistem *down*	AVA	C
22	Melaksanakan mekanisme enkripsi (data, *end-to-end*) untuk mencegah akses yang tidak sah untuk melindungi integritas sebuah kerahasiaan informasi.	6	Otorisasi keaslian permintaan data	INT	B
		20	Kesalahan terhadap data/ dokumen yang dipublikasikan	INT	C
		21	Informasi dari mitra atau pemasok terjadi kesalahan	INT	C
		27	Akses yang tidak terkendali terhadap informasi yang rahasia	CON	D
		28	Informasi sensitif dan tidak sensitif menjadi satu	CON	D

23	Merancang dan menerapkan pengendalian aplikasi (pengecekan pemasukan data lapangan yang memerlukan validasi, indikator alarm, kemampuan sandi kadaluarsa, pengecekan jumlah) untuk menjamin integritas, kerahasiaan, dan ketersediaan informasi aplikasi.	20	Kesalahan terhadap data/ dokumen yang dipublikasikan	INT	C
		28	Informasi sensitif dan tidak sensitif menjadi satu	CON	D
		38	Kesalahan terhadap instalasi *software*/*hardware*	AVA	C
24	Mengembangkan prosedur pengujian yang harus diikuti selama aplikasi dan selama modifikasi aplikasi yang sudah ada yang mencakup penggunaan partisipasi dan penerimaan.	8	Penggunaan informasi yang tidak benar yang dapat berdampak pada bisnis	INT	C
		18	Data lama/dokumen tidak dihapus	INT	C
		38	Kesalahan terhadap instalasi *software*/*hardware*	AVA	C
25	Mematuhi suatu proses perubahan manajemen yang dirancang untuk memfasilitasikan pendekatan struktur untuk modifikasi, untuk memastikan langkah yang tepat dan tindakan pencegahan akan dipatuhi. Modifikasi yang dilakukan secara mendesak harus dimasukan dalam proses ini.	4	Data diperbarui secara *internal* tapi tidak dibuat eksternal	INT	C
		5	Informasi pihak ketiga dapat menyebabkan masalah kepada perusahaan	INT	C
		7	Penolakan akses ke informasi padahal diakses oleh orang yang berwenang	INT	C
		15	Personil *internal* sengaja memodifikasi data untuk pribadi/keuntungan kelompok	INT	C
		17	Tidak adanya rekaman terhadap perubahan sistem/aplikasi *software*	INT	C
		19	Modifikasi anti virus terhadap perkembangan virus	INT	C
		23	Salah pengelompokan informasi/data	CON	C
		24	Akses terhadap pelanggan/mitra kerja tidak tersedia secara lengkap	CON	D
		25	Mantan *user*/ karyawan masih memiliki akses untuk mengamankan data	CON	C

		26	Menggunakan sistem yang rentan untuk mengirim data/ informasi yang penting	CON	D
		30	Penyalahgunaan *user* ID	CON	C
		31	Akses untuk *backup* data tidak terkontrol dengan baik	CON	D
		34	*Hacker* dapat membuat sistem *down*	AVA	C
		42	Terdapatanya virus dapat menyebabkan kegagalan sistem/ hilangnya data	AVA	C
26	Memastikan administrator LAN menginstal anti-virus perangkat lunak standar perusahaan di semua komputer. Serta adanya pelatihan dan kesadaran teknik pencegahan virus yang digabungkan dalam program organisasi.	6	Otorisasi keaslian permintaan data	INT	B
		11	Kurangnya personil dibidang sistem aplikasi	INT	C
		12	Informasi dikeluarkan tanpa otorisasi yang tepat	INT	C
		19	Modifikasi anti virus terhadap perkembangan virus	INT	C
		22	Informasi/ data tidak benar	CON	C
		28	Informasi sensitif dan tidak sensitif menjadi satu	CON	D
27	Mengembangkan kebijakan dan prosedur untuk membatasi akses dan mengoperasikan hak istimewa bagi mereka yang membutuhkan bisnis.	1	Informasi diakses oleh pihak yang tidak berwenang	INT	C
		5	Informasi pihak ketiga dapat menyebabkan masalah kepada perusahaan	INT	C
		7	Penolakan akses ke informasi padahal diakses oleh orang yang berwenang	INT	C
		8	Penggunaan informasi yang tidak benar yang dapat berdampak pada bisnis	INT	C
		11	Kurangnya personil dibidang sistem aplikasi	INT	C
		12	Informasi dikeluarkan tanpa otorisasi yang tepat	INT	C
		16	Tidak adanya kepercayaan bisnis dengan mitra pihak ketiga	INT	C
		19	Modifikasi anti virus terhadap perkembangan virus	INT	C

		21	Informasi dari mitra atau pemasok terjadi kesalahan	INT	C
		22	Informasi/ data tidak benar	CON	C
		28	Informasi sensitif dan tidak sensitif menjadi satu	CON	D
		33	Pihak ketiga membatalkan perjanjian yang telah dibuat	CON	C
		41	Kurangnya pelatihan bagi *user*	AVA	C
28	Pengguna pelatihan akan mencakup instruksi dan dokumentasi tentang penggunaan aplikasi secara benar. Pentingnya menjaga kerahasiaan dari account pengguna/ rekening pemakai, sandi, dan sifat rahasia dan kompetitif infoemasi akan ditekankan.	8	Penggunaan informasi yang tidak benar yang dapat berdampak pada bisnis	INT	C
		11	Kurangnya personil dibidang sistem aplikasi	INT	C
		12	Informasi dikeluarkan tanpa otorisasi yang tepat	INT	C
		14	Tidak menanggapi permintaan secara tepat waktu	INT	C
		19	Modifikasi anti virus terhadap perkembangan virus	INT	C
		21	Informasi dari mitra atau pemasok terjadi kesalahan	INT	C
		22	Informasi/ data tidak benar	CON	C
		37	Desain sistem terlalu rumit	AVA	C
29	Melaksanakan mekanisme untuk memantau/ mengawasi, melaporkan, dan kegiatan audit yang diidentifikasi sebagai yang memerlukan tinjauan independen, termasuk tinjauan berkala *user* ID untuk memastikan dan memverifikasi kebutuhan bisnis.	2	Kurangnya proses *internal* untuk membuat dan mengendalikan, mengelola data di seluruh fungsi	INT	C
30	Kontrol operasi adalah pelatihan untuk cadangan ke sistem administrator akan disediakan dan tugas diputar diantara mereka untuk memastikan kecukupan/ kemampuan dari program pelatihan.	8	Penggunaan informasi yang tidak benar yang dapat berdampak pada bisnis	INT	C
		28	Informasi sensitif dan tidak sensitif menjadi satu	CON	D
		41	Kurangnya pelatihan bagi *user*	AVA	C
31	Operasi pengendalian: pengembangan aplikasi akan memberikan dokumentasi, bimbingan, dan dukungan untuk staff operasi dalam melaksanakan mekanisme untuk memastikan bahwa transfer informasi antara aplikasi aman.	8	Penggunaan informasi yang tidak benar yang dapat berdampak pada bisnis	INT	C

		10	Proses kontrol yang terlalu rumit	INT	C
		37	Desain sistem terlalu rumit	AVA	C
32	Operasi Kontrol: Mekanisme untuk melindungi terhadap resiko database yang tidak sah, dan modifikasi yang dilakukan dari luar aplikasi, akan ditentukan dan diimplementasikan.	2	Kurangnya proses *internal* untuk membuat dan mengendalikan, mengelola data di seluruh fungsi	INT	C
		21	Informasi dari mitra atau pemasok terjadi kesalahan	INT	C
33	Operasi Kontrol: Sistem yang memberikan informasi akan diidentifikasi dan dikomunikasikan ke penyedia layanan untuk menekankan dampak terhadap fungsi jika pengisian aplikasi ini tidak tersedia.	37	Desain sistem terlalu rumit	AVA	C
		43	*Router* yang tidak berfungsi dengan baik dapat menyebabkan sulitnya akses pada layanan	AVA	C
34	Operasi Kontrol: Waktu persayaratan untuk pemeliharaan teknis akan dilacak dan permintaan untuk penyesuaian akan dikomunikasikan kepada manajemen jika diberikan jaminan.	9	Prosedur otorisasi pada perusahaan	INT	B
		11	Kurangnya personil dibidang sistem aplikasi	INT	C
		12	Informasi dikeluarkan tanpa otorisasi yang tepat	INT	C
		14	Tidak menanggapi permintaan secara tepat waktu	INT	C
		29	Otentikasi untuk akses informasi sensitif tidak memadai	CON	D
		39	Kebutuhan *backup* tidak memadai	AVA	D
		40	Konfigurasi *hardware* yang tidak memadai	AVA	D
35	Kontrol Pengguna: melaksanakan program pengguna (pengguna evaluasi kinerja) yang dirancang untuk mendorong kepatuhan terhadap kebijakan dan prosedur untuk memastikan penggunaan aplikasi yang tepat.	10	Proses kontrol yang terlalu rumit	INT	C
		35	Situs *hosting* tidak memiliki perlindungan fisik informasi	AVA	C
		43	*Router* yang tidak berfungsi dengan baik dapat menyebabkan sulitnya akses pada layanan	AVA	C

36	Perjanjian tingkat memperoleh layanan adalah untuk menetapkan tingkat harapan pelanggan dan jaminan dari mendukung operasi.	2	Kurangnya proses *internal* untuk membuat dan mengendalikan, mengelola data di seluruh fungsi	INT	C
		14	Tidak menanggapi permintaan secara tepat waktu	INT	C
		16	Tidak adanya kepercayaan bisnis dengan mitra pihak ketiga	INT	C
		34	*Hacker* dapat membuat sistem *down*	AVA	C
37	Memperoleh pemeliharaan atau perjanjian penyaluran/ penyedia untuk memfasilitasi berkelanjutan status operasional aplikasi.	21	Informasi dari mitra atau pemasok terjadi kesalahan	INT	C
		27	Akses yang tidak terkendali terhadap informasi yang rahasia	CON	D
		34	*Hacker* dapat membuat sistem *down*	AVA	C
		35	Situs *hosting* tidak memiliki perlindungan fisik informasi	AVA	C
		43	*Router* yang tidak berfungsi dengan baik dapat menyebabkan sulitnya akses pada layanan	AVA	C
38	Dalam konsultasi dengan manajemen fasilitas, memfasilitasi pelaksanaan kontrol keamanan fisik yang dirancang untuk melindungi informasi, perangkat lunak dan perangkat keras yang membutuhkan sistem.	9	Prosedur otorisasi pada perusahaan	INT	B
		13	Kebocoran informasi *internal* perusahaan	INT	C
		16	Tidak adanya kepercayaan bisnis dengan mitra pihak ketiga	INT	C
		29	Otentikasi untuk akses informasi sensitif tidak memadai	CON	D
		32	Keamanan *firewall* diintrusi	CON	D
39	Permintaan dukungan manajemen untuk menjamin kerjasama dan koordinasii berbagai unit bisnis, untuk memfasilitasi kelancaran transisi ke aplikasi.	12	Informasi dikeluarkan tanpa otorisasi yang tepat	INT	C
40	Kepemilikan kontrol.	1	Informasi diakses oleh pihak yang tidak berwenang	INT	C
		3	Informasi digunakan dalam konteks yang tidak sesuai	INT	C
		9	Prosedur otorisasi pada perusahaan	INT	B

41	Tim pengembang akan mengembangkan strategi korektif seperti proses ulang, merevisi/ merubah logika aplikasi, dll.	8	Penggunaan informasi yang tidak benar yang dapat berdampak pada bisnis	INT	C
		18	Data lama/dokumen tidak dihapus	INT	C
		20	Kesalahan terhadap data/ dokumen yang dipublikasikan	INT	C
42	Produksi kontrol migrasi seperti pencarian dan menghapus/ menghilangkan proses untuk memastikan penyimpanan data yang bersih.	31	Akses untuk *backup* data tidak terkontrol dengan baik	CON	D
43	Melakukan pemerikasaan secara rutin (berkala) terhadap hardware, software, dan sistem informasi yang ada.	4	Data diperbarui secara *internal* tapi tidak dibuat eksternal	INT	C
		9	Prosedur otorisasi pada perusahaan	INT	B
		12	Informasi dikeluarkan tanpa otorisasi yang tepat	INT	C
		13	Kebocoran informasi internal perusahaan	INT	C
		17	Tidak adanya rekaman terhadap perubahan sistem/aplikasi *software*	INT	C
		18	Data lama/dokumen tidak dihapus	INT	C
		19	Modifikasi anti virus terhadap perkembangan virus	INT	C
		22	Informasi/ data tidak benar	CON	C
		26	Menggunakan sistem yang rentan untuk mengirim data/ informasi yang penting	CON	D
		29	Otentikasi untuk akses informasi sensitif tidak memadai	CON	D
		31	Akses untuk *backup* data tidak terkontrol dengan baik	CON	D
		32	Keamanan *firewall* diintrusi	CON	D
		34	*Hacker* dapat membuat sistem *down*	AVA	C
		35	Situs *hosting* tidak memiliki perlindungan fisik informasi	AVA	C
		36	Hubungan jaringan antar sistem gagal didalam perusahaan	AVA	C
		38	Kesalahan terhadap instalasi *software*/*hardware*	AVA	C

Implementasi Kontrol terhadap Resiko-resiko yang Masih Terbuka

Pada tahap ini pimpinan proyek dan fasilitator akan bertemu dengan manajer bisnis untuk meninjau ulang, mengidentifikasi kontrol apa saja yang dapat digunakan untuk mengatasi resiko-resiko yang masih terbuka. Menentukan *control* apa saja yang perlu dilakukan untuk menganggulangi resiko yang masih terbuka. Atau bahwa ternyata resiko tersebut tidaklah bersifat *high impact* sehingga bisnis manajer mengindikasikan resiko tersebut sebagai resiko yang dapat diterima.

PENUTUP

Melalui pendekatan FRAP terhadap proses penentuan resiko dan dampaknya, proses penentuan prioritas, dan proses penentuan kontrol pengamanan proses analisis resiko dapat dilakukan dalam hitungan hari, bukan mingguan atau bulanan. Dengan demikian analisis resiko bukan merupakan kendala, tetapi proses yang sangat mungkin dilakukan dan juga diperlukan. Di samping tidak begitu sulit untuk dilakukan, dengan pendekatan FRAP pemilik resiko turut serta dalam hal penentuan resiko dan prioritas resiko yang membuat pengukuran resiko menjadi lebih fokus dan terarah. Simpulan yang dapat diambil dari hasil penelitian di antaranya adalah: (1) penerapan teknologi informasi sudah memiliki peranan yang penting di dalam perusahaan; (2) perusahaan telah mengelola sistem keamanan jaringan dengan baik, ini dikarenakan jaringan perusahaan telah dipantau dan diaudit secara rutin. Walaupun ada sesekali kerusakan yang terjadi tetapi ini dapat ditanggulangi dengan baik; Kurangnya pengendalian internal dalam perusahaan, dalam hal pembuatan prosedur sistem aplikasi, yang saat ini sedang dalam proses pengembangan; (3) perusahaan sebaiknya membuat dokumentasi terhadap *Disaster recovery Plan* (DRP), untuk memudahkan perusahaan dalam menangani resiko yang muncul. Informasi dan sistem yang menjadi proses sumber daya ini adalah aset yang sangat penting dan utama untuk mendukung bisnis atau misi dari perusahaan apapun dan harus dilindungi. Suatu proses analisis resiko yang efektif menjamin bahwa kebutuhan bisnis dipenuhi.

DAFTAR PUSTAKA

Djojosoedarso, S. (2005). *Prinsip-prinsip Manajemen Resiko Asuransi* (edisi revisi). Jakarta: Salemba Empat.

Gondodiyoto, Sanyoto. (2009). *Pengelolaan Fungsi Audit Sistem Informasi* (edisi ke-2). Jakarta: Mitra Wacana Media.

O'Brien, James A. & Marakas, George M. (2007). *Management Information Systems* (edisi ke-7). New York: McGraw-Hill.

Peltier, Thomas R. (2001). *Information security Risk Analysis*. Washington D.C: Auerbach/CRC Press.