Evaluasi Sistem informasi Dalam Organisasi Berdasarkan pendekatan Facilitated Risk Analysis and Assessment Process

Firmansyah
Balai Pendidikan dan pelatihan
Tambang Bawah Tanah

Wahyu Indra Satria
Faculty Of Computer Science
University Of Indonesia
Depok, Indonesia
wahyu.indra51@ui.ac.id

1. LATAR BELAKANG

Teknologi informasi saat ini telah berkembang pesat. Melalui teknologi informasi, manusia dapat mengakses informasi yang dibutuhkan dalam waktu singkat dan dengan cara lebih praktis. Oleh karena itu, teknologi informasi memiliki peranan besar, khususnya dalam mendukung kinerja aktivitas kehidupan manusia. Hidup dan matinya setiap organisasi pada jaman sekarang ini ditentukan oleh penyimpanan data pada komputer dan jaringan, serta tidak ada organisasi yang dapat bertahan hidup jika data yang dimilikinya tidak akurat dan terpercaya. "*Every enterprise now lives and dies by the data stored on its computers and networks, and none can long survive if that data isn't accurate and reliable. In addition to the damage that can come from the actual alteration of data, the impact on a company's reputation can be substantial if customers are faced with unreliable, poor quality products"* (Voas & Wilbanks, 2008). Dengan perkembangan pesat tersebut, teknologi informasi juga mengambil peranan penting dalam siklus proses kehidupan akademis, pada hampir seluruh institusi pendidikan, sehingga kemajuan yang ada di dalam dunia pendidikan saat ini, membuat institusi pendidikan tersebut menargetkan untuk dapat memiliki kemajuan di bidang teknologi informasi, dikarenakan peranan dari teknologi informasi dapat menghasilkan suatu informasi yang cepat, tepat, dan dapat diandalkan untuk mendukung kegiatan operasional institusi pendidikan.

Pada zaman sekarang ini, kelangsungan hidup suatu institusi pendidikan tergantung oleh penyimpanan data pada komputer dan jaringan. Kelangsungan hidup suatu institusi pendidikan tidak akan bisa bertahan jika data yang dimilikinya belum

diproses secara akurat. Dapat diambil kesimpulan bahwa jika setiap institusi pendidikan ingin mempertahankan dan meningkatkan pelayanannya terhadap sivitas akademika, sebuah institusi pendidikan harus memiliki penyimpanan data pada komputer dan jaringan secara akurat.

Banyak institusi pendidikan memanfaatkan teknologi informasi dan membangun sistem informasi pada proses pelayanan sivitas akademika yang berjalan, sehingga teknologi informasi dan sistem informasi telah menjadi suatu komponen yang tidak terpisahkan dalam dunia pendidikan di era globalisasi saat ini. "*IT implementation needs to be well managed in order to produce quality information for the stakeholders and give a competitive advantage for higher organization*" (Maria, 2012). Pengimplementasian teknologi informasi di dalam suatu institusi pendidikan perlu dikelola dengan baik agar dapat menghasilkan informasi yang berkualitas bagi para sivitas akademika dan memberikan keunggulan kompetitif bagi institusi pendidikan itu sendiri. Dari pernyataan tersebut, dapat diambil kesimpulan bahwa tata kelola teknologi informasi yang baik dapat membantu institusi pendidikan dalam mempertahankan dan meningkatkan pelayanan kepada para sivitas akademika. Mengacu kepada hal tersebut, maka akan melakukan audit sistem informasi pada dalam Organisasi.

2. TUJUAN

Tujuan perencanaan audit berbasis aplikasi sistem informasi pada Organisasi adalah:

1. Melakukan analisa dan evaluasi terhadap penerapan aplikasi pada proses pelayanan pendidikan terhadap pegawai di organisasi.
2. Mengidentifikasi dan mengevaluasi resiko yang terjadi terkait dengan pengimplementasian aplikasi pada proses pelayanan pendidikan terhadap pegawai di organisasi.
3. Memberikan rekomendasi perbaikan dan pengendalian resiko pada kegiatan proses pelayanan berjalan yang berkaitan dengan aplikasi, berkenaan dengan proses pelayanan.

3. PENILAIAN RESIKO

Berikut ini adalah tabel resiko yang mungkin dapat terjadi pada area audit, beserta dengan tingkatan (*level*) resiko bagi keberlangsungan bisnis organisasi, dan

pengendalian (*control*) terkait dengan resiko tersebut.

Tabel 4.1 Penilaian Resiko

No.	Resiko	Tingkatan (*Level*) Resiko	Pengendalian (*Control*)
1.	Informasi diakses oleh pihak yang tidak berwenang	Menengah	Pengendalian Keamanan Akses
2.	Data dan informasi tidak sesuai dengan fakta	Tinggi	Pengendalian Manajemen Perubahan Data dan Informasi
3.	Kehilangan data dan informasi akibat kebakaran	Tinggi	Pengendalian *Back-up System*
4	Tidak ada peringatan atas kesalahan *input* data	Rendah	Pengendalian Aplikasi
5.	Kegagalan sistem dan hilangnya data akibat *virus* komputer	Tinggi	Pengendalian Aplikasi
6.	Manipulasi data untuk kepentingan pribadi atau kelompok	Tinggi	Pengendalian Pengguna (*User*)
7.	*Human error* pada saat melakukan input data	Rendah	Pengendalian Pengguna (*User*)
8.	Kerusakan *hardware* akibat kebakaran	Tinggi	Pengendalian Pemeliharaan
9.	Penolakan akses ke informasi oleh pihak yang memiliki otorisasi	Menengah	Pengendalian Operasi Sistem
10.	Kerusakan *database*	Tinggi	Pengendalian Pemeliharaan
11.	Membuat laporan yang salah	Rendah	Pengendalian Pengguna (*User*)
12.	Mantan user atau karyawan masih memiliki akses terhadap data dan informasi	Menengah	Pengendalian Manajemen Perubahan Data dan Informasi
13.	Adanya resiko duplikasi Informasi perusahaan	Menengah	Pengendalian Aplikasi
14.	Kebocoran informasi internal perusahaan	Menengah	Pengendalian Keamanan Akses
15.	Gangguan jaringan akibat virus komputer	Tinggi	Pengendalian Operasi Sistem
16.	Berbagi *user ID*	Rendah	Pengendalian Pengguna (*User*)
17.	*Hacker* dapat membuat sistem down	Tinggi	Pengendalian Operasi Sistem

18.	Hubungan jaringan antar sistem gagal didalam perusahaan	Tinggi	Pengendalian Operasi Sistem
19.	Kegagalan *router* atau *firewall* membuat layanan tidak dapat diakses	Tinggi	Pengendalian Pemeliharaan
20.	*Error* pada program	Tinggi	Pengendalian Aplikasi
21.	Putusnya koneksi internet	Menengah	Pengendalian Pemeliharaan
22.	Kesalahan dalam membuat perubahan *software*	Tinggi	Pengendalian Aplikasi
23.	Informasi yang diakses tidak tersedia	Tinggi	Pengendalian Manajemen Perubahan Data dan Informasi

4. RUANG LINGKUP AUDIT

Dalam melaksanakan audit, auditor membatasi ruang lingkup perencanaan proses audit yang akan dilakukan, yaitu:

1. Audit dilaksanakan pada organisasi.
2. Audit dilaksanakan pada Salah satu Aplikasi
3. Fokus pengumulan dokumen dan bukti audit, hanya pada Salah satu Aplikasi.
4. Batasan fokus pengendalian audit yang akan dilaksanakan:
    a. Pengendalian Keamanan Akses.
    b. Pengendalian Manajemen Perubahan Data dan Informasi.
    c. Pengendalian *Back-up System*
    d. Pengendalian Pengguna (*User*)
    e. Pengendalian Operasi Sistem
    f. Pengendalian Pemeliharaan
    g. Pengendalian Aplikasi

5. METODOLOGI DAN KRITERIA AUDIT

Metodologi dan kriteria audit yang akan dilaksanakan oleh auditor adalah sebagai berikut:

- **Tahap Pertama, Melakukan Pertemuan Dengan Manajemen Tingkat Atas.**
  Pada tahap ini, tim auditor melakukan kunjungan kepada pihak *auditee*, untuk melaksanakan penandatanganan Surat Perikatan Audit (*Audit Engagement Letter*) sebagai dasar dari tindakan audit yang akan dilakukan serta sebagai bukti otentik persetujuan pelaksanaan audit antara auditor dengan *auditee*.

- **Tahap Kedua, Melakukan Wawancara Dengan Pihak - Pihak Yang Terkait Dengan Kegiatan Audit.**
  Setelah perjanjian audit disepakati, maka tim auditor akan melaksanakan wawancara dengan pihak – pihak yang terkait dengan kegiatan audit untuk mengumpulkan seluruh data penting yang dibutuhkan dalam melakukan audit.

- **Tahap Ketiga, Mendokumentasikan Data Penting Yang Didapatkan.**
  Tim auditor melakukan dokumentasi data penting yang dibutuhkan dalam melaksanakan audit, seperti profil organisasi, visi misi, struktur orgnisasi, penilaian resiko yang mungkin dapat terjadi pada area audit, beserta dengan tingkatan (*level*) resiko bagi keberlangsungan bisnis organisasi, dan pengendalian (*control*) terkait dengan resiko tersebut, juga data penting lainnya.

- **Tahap Keempat, Melakukan Analisis Terhadap Informasi Yang Didapatkan.**
  Pada tahap ini, tim auditor akan mengolah data yang di dapatkan untuk diformulasikan dengan menggunakan kriteria audit acuan yaitu FRAAP. "FRAAP (*Facilitated Risk Analysis and Assessment Process*), Proses Penilaian dan Analisa Resiko yang Difasilitasi, telah dikembangkan sebagai suatu proses yang efisien dan teratur, serta digunakan untuk memastikan bahwa resiko terkait dengan keamanan informasi proses bisnis, telah dianalisa dan didokumentasikan. Pada berjalannya proses tersebut, melibatkan analisa suatu sistem aplikasi yang saling terkait. (Peltier, 2005)"

- **Tahap Kelima, Pelaksanaan Audit Dan Pelaporan.**

  Pada tahap ini, tim auditor akan melaksanakan audit dan juga melakukan dokumentasi (pelaporan) terhadap hasil audit, guna memberikan rekomendasi perbaikan dan pengendalian resiko pada kegiatan proses pelayanan berjalan yang berkaitan dengan salah satu aplikasi, berkenaan dengan proses pelayanan di organisasi.

Reference

Boediman, A. (2012). *Evaluasi Pengelolaan Obat di Instansi Farmasi Rumah Sakit (Studi Kasus Rumah Sakit Karya Bhakti Bogor)* .

Hardcastle, E. (2011). *Business Information Systems.* Ventus Publishing ApS.

Ikafitriani, A. (2012). *EVALUASI PERENCANAAN DAN KETERSEDIAAN OBAT DI RUMAH SAKIT JIWA GRHASIA PROVINSI DAERAH ISTIMEWA YOGYAKARTA TAHUN 2009 – 2010* .

Ivancovic, D. (2008). *Analysis of Data as Information* .

Kusumadianti. (2011). Peranan Sistem Pengendalian Internal Terhadap Efektivitas Persediaan Obat-Obatan pada RSUD dr.ISKAK TULUNGAGUNG.

M.Stair, R., & G. R. (2010). *Principles of Information System.* Course Technology Cengage Learning.

Maria. (2012). *THE MEASUREMENT OF INFORMATION TECHNOLOGY PERFORMANCE IN INDONESIAN* .

Peltier, T. R. (2005). *Information Security Risk Analysis.* CRC Press.

Rama, D. V., & Jones, F. L. (2008). *Sistem Informasi Akuntansi.* Salemba Empat.

Umar. (2008). *Evaluasi Sistem Informasi* , 25.

Voas, J., & Wilbanks, L. (2008). *Information and Quality Assurance, An Unsolved, Perpetual Problem for Past and Future Generations* , 10-13.

Whitman, M., & Mattord, H. (2010). *Management Of Information Security.* Course Technology.