Information Technology Risk Assessment Sistem Informasi Elektronik Kinerja Pegawai Universitas Islam Negeri

Muhammad Leandry Dalafranka[1], Dedy Syamsuar[2], Yesi Novaria Kunang[3]

Fakultas Ilmu Komputer Universitas Bina Darma
Universitas Islam Negeri Raden Fatah Palembang
email : leandry_uin@radenfatah.ac.id[1], dedy_syamsuar@binadarma.ac.id[2], yesinovariakunang@binadarma.ac.id[3]
Jl. A. Yani No. 3, Palembang 30624, Indonesia

Abstrak

Berkembangannya teknologi yang membantu memenuhi infomasi sudah diterapkan pada Universitas Islam Negeri Raden Fatah Palembang dimana ada beberapa sistem yang sangat penting, seperti: seperti Sistem Informasi Elektronik Laporan Kinerja Pegawai UIN Raden Fatah Palembang. Dengan sistem yang telah dipakai pada setiap unit-unit kerja dapat dilihat bahwa IT merupakan salah satu faktor penting dalam mendukung pekerjaan dan jika salah satu sistem sebut tidak online, maka pegawai atau mahasiswa terhambat pekerjaannya dan jika sistem tidak online dalam waktu lama dapat membuat semua pekerjaan terhenti dan merugikan dari sisi waktu dan materi. Sistem informasi yang dimiliki oleh Universitas Islam Negeri Raden Fatah Palembang merupakan aset yang berharga. Berkembangnya teknologi sering kali dimanfaatkan oleh beberapa pihak yang tidak bertanggung jawab yang dapat menyebabkan munculnya ancaman dan risiko dari penggunaan teknologi. Dengan menggunakan tahapan risk assessment dalam Framework NIST SP 800-30 Rev 1 untuk mengetahui dan menganalisis risiko yang ada pada penerapan Sistem Elektronik Laporan Kinerja Pegawai di Universitas Islam Negeri Raden Fatah Palembang sehingga menghasilkan laporan risiko teknologi informasi pada penerepan sistem tersebut.

Kata kunci: *Information technology*, nist sp 800-30 rev 1 dan *risk assessment*.

1. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) yang sangat pesat dewasa ini memberikan banyak kemudahan pada berbagai aspek kegiatan bisnis, Peranan TI dalam berbagai aspek dapat dipahami karena sebagai sebuah teknologi yang menitik beratkan pada pengaturan sistem informasi dengan penggunaan komputer, teknologi informasi dapat memenuhi kebutuhan informasi dengan sangat cepat, tepat waktu, relevan, dan akurat (Rahadi, 2007).

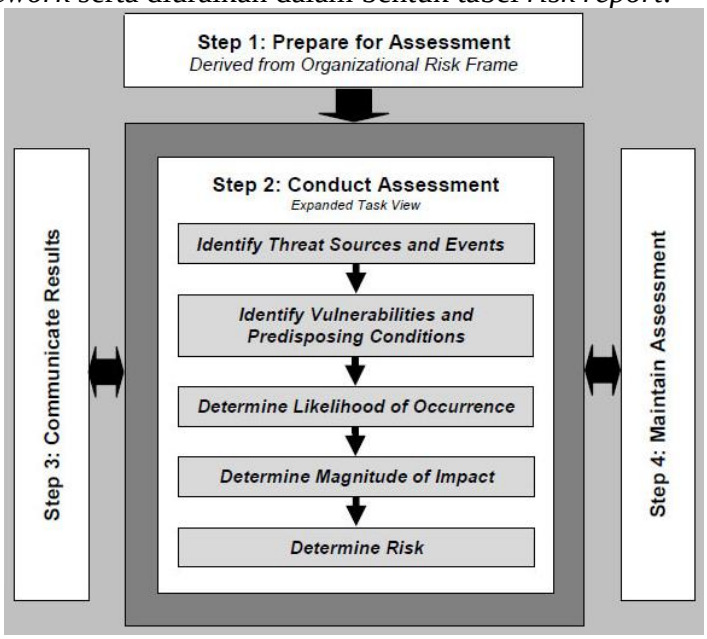
Berkembangannya teknologi yang membantu memenuhi infomasi sudah diterapkan pada Universitas Islam Negeri Raden Fatah Palembang dimana ada beberapa sistem yang sangat penting yang salah satunya adalah Sistem Informasi Elektronik Laporan Kinerja Pegawai (E-LKP). Dengan banyaknya sistem yang telah dipakai pada setiap unit-unit kerja dapat dilihat bahwa IT merupakan salah satu faktor penting dalam mendukung pekerjaan dan jika salah satu sistem sebut tidak online, maka pegawai atau mahasiswa terhambat pekerjaannya dan jika sistem tidak online dalam waktu lama dapat membuat semua pekerjaan terhenti dan merugikan dari sisi waktu dan materi.

Untuk sebagian besar institusi, informasi dan teknologi yang mendukung kegiatan Perguruan Tinggi merupakan aset yang berharga. Perguruan Tinggi yang sukses biasanya memahami keuntungan dan kegunaan dari teknologi informasi untuk mendukung kinerja Perguruan Tinggi (Setiawan, 2009). Perguruan Tinggi seringkali menggunakan Teknologi Informasi sebagai pendukung dalam mengelola informasi sebagai basis dalam penciptaan layanan yang berkualitas ataupun dalam optimalisasi proses bisnisnya. Meningkatnya tingkat ketergantungan organisasi pada sistem informasi sejalan dengan risiko yang mungkin timbul, sedangkan pihak universitas belum pernah melakukan penilaian risiko pada implementasi sistem informasi yang ada dengan menggunakan metode atau kerangka kerja tertentu. Salah satu risiko yang timbul adalah risiko keamanan informasi, dimana informasi menjadi suatu hal yang penting yang harus tetap tersedia dan dapat digunakan. Selain itu juga terjaga keberadaannya dari pihak yang tidak berwenang, baik dari pihak luar maupun dalam yang akan memanfaatkannya untuk kepentingan tertentu atau bahkan akan merusak informasi tersebut. Informasi merupakan sebuah aset penting bagi Perguruan tinggi yang perlu dilindungi dan diamankan, sehingga menjamin ketersediaan informasi yang berguna dan dapat dipercaya baik oleh lingkungan internal maupun eksternal (Nugraha, 2016).

Pada kenyataannya sistem yang ada pada UIN Raden Fatah Palembang masih belum dapat perhatian tentang keamanan informasi serta risiko-risiko yang mungkin akan timbul dan bagaimana menajemennya, sehingga karena kurangnya perhatian tersebut terdapat beberapa risiko yang pernah timbul, contoh kasus yang terakhir adalah kerusakan sistem E-Remunerasi, sistem itu sendiri berisi data, penilaian, sekaligus perhitungan insentif pegawai dan dosen dengan melihat indeks kinerjanya. Dengan rusaknya sistem tersebut maka pembayaran remunerasi pegawai dan dosen menjadi terhambat sampai waktu yang tidak ditentukan.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan *assessment* dari *framework nist sp 800-30 rev 1* dengan data hasil dari wawancara dan kuisioner. Selanjutnya data yang telah diperoleh akan diolah berdasarkan *framework* serta diuraikan dalam bentuk tabel *risk report*.



Sumber: NIST SP 800-30 Rev 1, 2010.

Gambar 1 Risk Assessment (NIST SP 800-30 Rev 1)

1. Persiapan Untuk Penilaian

Langkah pertama dalam proses penilaian risiko adalah mempersiapkan penilaian. Tujuan dari langkah ini adalah untuk menetapkan konteks penilaian risiko.

2. Melakukan Penilaian
   Langkah kedua dalam proses penilaian risiko adalah melakukan penilaian. Tujuan dari langkah ini adalah untuk menghasilkan daftar risiko keamanan informasi yang dapat diprioritaskan oleh tingkat risiko dan digunakan untuk menginformasikan keputusan respons risiko. Untuk mencapai tujuan ini adapun tahapannya berupa identifikasi terhadap sumber ancaman (*identification of threat sources)*, identifikasi peristiwa ancaman (*identification of threat events*), identifikasi kerentanan (*identification of vulnerabilites*), identifikasi kondisi yang mempengaruhi (*identification of predisposing conditions*), kemungkinan keseluruhan (*overall likehood*), identifikasi dampak merugikan (*identification of adverse impacts*), dan tingkat risiko (*level of risk*).
3. Komunikasi dan Berbagi Informasi Penilaian Risiko
   Langkah ketiga dalam proses penilaian risiko adalah mengkomunikasikan hasil penilaian dan berbagi informasi terkait risiko. Tujuan dari langkah ini adalah untuk memastikan bahwa pengambil keputusan di seluruh organisasi memiliki informasi terkait risiko yang sesuai yang diperlukan untuk menginformasikan dan membimbing keputusan risiko.
4. Mempertahankan Penilaian Risiko
   Langkah keempat dalam proses penilaian risiko adalah mempertahankan asesmen. Tujuan dari langkah ini adalah untuk menjaga arus, pengetahuan spesifik dari organisasi yang terdapat risiko. Hasil penilaian risiko menginformasikan keputusan manajemen risiko dan memandu tanggapan risiko. Untuk mendukung peninjauan kembali keputusan manajemen risiko yang sedang berlangsung (contoh: Keputusan akuisisi, keputusan otorisasi untuk sistem informasi dan kontrol umum, keputusan koneksi), organisasi mempertahankan penilaian risiko untuk menggabungkan setiap perubahan yang terdeteksi melalui pemantauan risiko.

2.1 Teknik Pengumpulan Data

Teknik yang dapat digunakan dalam mengumpulkan informasi yang relevan dengan sistem TI dalam batas operasionalnya sebagai berikut (Stoneburner, Goguen, & Feringa, 2002) antara lain wawancara, dengan personil dukungan sistem dan manajemen TI dapat memungkinkan personil penilaian risiko mengumpulkan informasi bermanfaat tentang sistem TI (mis., Bagaimana sistem dioperasikan dan dikelola). Dalam hal ini bidang yang menjadi objek wawancara adalah 3 (tiga) orang informan, yaitu Kepala Pusat Teknologi Informasi dan Pangkalan Data (PUSTIPD), divisi pengembangan sistem dan divisi jaringan. Waktu penelitian dilakukan di Universitas Islam Negeri Raden Fatah Palembang selama 8 bulan dimulai pada November 2017 sampai dengan bulan Mei 2018.

3. HASIL DAN PEMBAHASAN

Penelitian Nurcahyo (2013) melakukan evaluasi pelaksanaan manajemen risiko tekologi teknologi informasi pada kantor arsip daerah Kota Samarinda dengan menggunakan *Framework Risk IT* untuk mengevaluasi pelaksanaan manajemen risiko teknologi informasi yang ada dengan tujuan untuk meminimalkan risiko yang mungkin akan timbul dan hasil dari penelitian ini memberikan informasi tentang kondisi tingkat kematangan sistem pada Domain Tata Kelola Risiko, Evaluasi Risiko dan Respon Risiko. Kemudian pada penelitian Budiarto (2017) melakukan penerapan Metode FMEA *(Failure Mode & Effect Analysis)* untuk keamanan sistem informasi website polri untuk tujuan untuk mengeksplorasi penggunaan metode FMEA pada sistem informasi serta mengidentifikasi potensi gangguan

dan permasalahan yang ada pada sistem informasi website Polri dan hasil dari penelitian ini telah memberikan kontribusi teori terhadap pengukuran skala pada *variabel severity* dan *occurance* pada pengukuran RPN *(Risk Priority Number)* sehingga dapat diterapkan pada objek sistem informasi.

Melihat beberapa penelitian sebelumnya, bahwa sangat diperlukannya manajemen risiko yang baik pada suatu organisasi, agar dapat berjaga-jaga pada saat sistem mengalami masalah atau serangan dari dalam maupun luar organisasi. Dimana hasil dari analisis pada penelitian ini dapat dilihat pada Tabel 1 untuk risiko musuh dan Tabel 2 untuk risiko bukan musuh.

Tabel 1. Risiko Musuh

Ancaman	Tingkat Risiko
Menempatkan seseorang ke dalam posisi penting organisasi	Sangat Tinggi
Menempatkan seseorang / beberapa orang yang dapat mengganggu di dalam organisasi	Sangat Tinggi
Memasang sniffers dengan tujuan umum ke pengendalian sistem informasi organisasi	Tinggi
Mempersiapkan percobaan serangan *brute force login* untuk menebak *password* (jaringan)	Tinggi
Mempersiapkan serangan *Distributed Denial of Service* (DDoS)	Tinggi
Mempersiapkan serangan modifikasi lalu lintas jaringan eksternal	Tinggi
Mempersiapkan serangan modifikasi lalu lintas jaringan *internal*	Tinggi
Mengeksploitasi sistem informasi yang tidak dikonfigurasi dengan benar yang tersebar di internet	Tinggi
Menyabotase akses fisik dari staff berwenang untuk mendapatkan akses ke organisasi	Tinggi
Menyebabkan kerusakan data penting	Tinggi
Melakukan *sniffing* jaringan terbuka	Sedang
Melakukan pengintaian/pemindaian jaringan	Sedang
Memasang sniffers dengan tujuan umum ke pengendalian jaringan organisasi	Sedang
Memasang terus-menerus *sniffing* bertarget pada jaringan organisasi	Sedang
Memasang terus-menerus *sniffing* bertarget pada sistem informasi organisasi	Sedang
Membahayakan misi informasi penting	Sedang
Phishing Attacks	Sedang
Menjadikan "*Phishing Attacks*" sebagai tombak serangan	Sedang
Membuat situs palsu	Sedang
Mempersiapkan percobaan serangan *brute force login* untuk menebak *password* (sistem)	Sedang
Mempersiapkan serangan *Denial of Service (DoS)* bertarget	Sedang
Mempersiapkan serangan gangguan *wireless*	Sedang
Mempersiapkan serangan menggunakan port, protokol dan layanan yang tidak sah	Sedang
Mempersiapkan serangan penangkapan jalur komunikasi	Sedang
Mendapatkan data atau informasi sensitif dari sistem informasi yang dapat diakses publik	Sedang
Mendapatkan informasi sensitif melalui penyadapan jaringan eksternal	Sedang
Mengeksploitasi kerentanan yang sering ditemukan	Sedang
Menyebabkan kerusakan dari komponen dan fungsi sistem informasi penting	Sedang
Menyebabkan penurunan atau tidak dapat diakses pada layanan yang diserang	Sedang

Ancaman	Tingkat Risiko
Menempatkan kerusakan pada komponen sangat penting di sistem organisasi	Rendah
Membuat *certificates digital* palsu	Rendah
Mempersiapkan serangan *Denial of Service* (DoS) sederhana	Rendah
Mempersiapkan serangan bertarget dan membahayakan perangkat pribadi karyawan penting	Rendah
Mempersiapkan serangan yang memanfaatkan lalu lintas / perpindahan data yang dibolehkan untuk melintas	Rendah
Mempersiapkan teknik sosial dari *internal* organisasi untuk mendapatkan informasi	Rendah
Mengetahui desain, pembuatan, dan penyaluran perangkat sistem informasi (termasuk perangkat keras, perangkat lunak, dan firmware)	Rendah
Mengirim *malware* dengan menyediakan *removable media*	Rendah
Mengirim *malware* yang bertarget untuk mengendalikan sistem internal dan menyalin data secara ilegal	Rendah
Mengirim *malware* yang dikenal untuk sistem informasi organisasi internal (misalnya, virus melalui *email*)	Rendah
Mengumpulkan informasi menggunakan *open source* informasi organisasi	Rendah
Menyebabkan hilangnya kelengkapan sistem dengan membuat, merusak dan mengubah data yang ada pada sistem (misalnya, *Web Deface*)	Rendah

Sumber: data yang diolah

Tabel 2. Risiko Bukan Musuh

Ancaman	Tingkat Risiko
Penipisan sumber daya	Sangat Tinggi
Banjir di fasilitas *backup*	Tinggi
Banjir di fasilitas utama	Tinggi
Bocornya informasi sensitif	Tinggi
Disk error yang meluas	Tinggi
Peningkatan suhu perangkat jaringan	Tinggi
Disk error	Sedang
Kesalahan instalasi jaringan	Sedang
Kesalahan penanganan informasi kritis dan / informasi sensitif oleh pengguna berwenang	Sedang
Pengaturan hak istimewa yang salah	Sedang
Peningkatan suhu ruangan	Sedang
Boot error	Rendah
Error update sistem operasi	Rendah
Informasi tentang kerentanan di dalam produk *software*	Rendah

Sumber: data yang diolah

4. KESIMPULAN DAN SARAN

Dari penelitian yang telah dilakukan, ada beberapa kesimpulan yang dapat diambil sebagai berikut:

1. Setelah dilakukan analisis risiko diketahui bahwa dalam penerapan Sistem Elektronik Laporan Kinerja Pegawai di Universitas Islam Negeri Raden Fatah Palembang terdapat risiko yang berasal dari risiko musuh maupun risiko bukan musuh yang mana dapat mengganggu sistem kedepannya.
2. Dari apa yang dibahas dapat dilihat ternyata risiko yang menempati rating tertinggi adalah dari serangan musuh (orang luar) dengan melihat peristiwa ancaman yang teridentifikasi, kemudian ketidaksengajaan orang dalam yang dikarenakan kelalaian

atau kurangnya pengetahuan sistem, dan tegangan listrik dikarenakan faktor lingkungan sekitar dan ditambah backup daya yang belum tersedia, sehingga risiko tersebut sangat perlu diperhatikan untuk kedepannya.

Atas dasar kesimpulan diatas, maka saran yang dapat disampaikan sebagai berikut:

1. Dengan melihat risiko-risiko yang telah teridentifikasi, maka perlu untuk melakukan perbaikan atau pemulihan yang diantaranya adalah membuat Standar Operasional Prosedur (SOP) yang berhubungan dengan keamanan IT, selanjutnya memasang alat-alat pendukung IT seperti genset, firewall, secondary disk, dan berlangganan Secure Socket Layer (SSL), kemudian yang terakhir adalah pelatihan terhadap sumber daya manusia baik itu pegawai biasa (users) maupun admin (staff IT).
2. Untuk pengembangan penelitian yang akan datang, maka penulis menyarankan dilakukan risk assessement yang lebih mendalam dan beragam pada sistem informasi yang ada pada Universitas Islam Negeri Raden Fatah Palembang.

Referensi

Budiarto, R. (2017). Penerapan Metode FMEA Untuk Keamanan Sistem Informasi.

Nugraha, U. (2016). *Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja Nist SP 800-300*.

Nurcahyo, D. (2013). Evaluasi Pelaksanaan Manajemen Risiko Teknologi Informasi pada Kantor Arsip Daerah Kota Samarinda dengan Menggunakan The Risk IT Framework. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI), 2*(3).

Rahadi, D. R. (2007). *Peranan Teknologi Informasi dalam peningkatan pelayanan di sektor publik.* Paper presented at the Seminar Nasional Teknologi.

Setiawan, A. (2009). *Evaluasi penerapan teknologi informasi di perguruan tinggi swasta Yogyakarta dengan menggunakan model Cobit framework.* Paper presented at the Seminar Nasional Aplikasi Teknologi Informasi (SNATI).

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.