Jurnal Bina Komputer
JBK, Vol. 1, No. 1, Februari 2019: 54-60
Received: 5 Januari 2019; Revised: 29 Januari 2019; Accepted: 30 Januari 2019

ASSESSMENT RESIKO TEKNOLOGI PADA IMPLEMENTASI SISTEM INFORMASI AKADEMIK E-UNIVERSITY

Yayuk Ike Meilani[1], Dedy Syamsuar[2], Yesi Novaria Kunang[3]

Program Magister Teknik Informatika
Universitas Bina Darma
email :[1,2,3]yayuk_ike@palcomtech.ac.id, dedysyamsuar@binadarma.ac.id, yesinovariakunang@binadarma.ac.id
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstract

Information technology has become an essential part of human life so as to facilitate a business activity. However, the use of information technology is not separated from the risks that can affect the process of the activity. As for the purpose of this study was to conduct an assessment of risk against potential vulnerabilities and threats that can attack the academic information system E-University all at once mempersiapan action anticipation towards things that can interfere with the the system. To do the assessment, this study uses the framework NIST SP 800-30r-1 consisting of nine stages to risk assessment i.e. in the characteristics of the system are used, identify the threats that attack system, identification of vulnerability, control systems, determine the likelihood of occurring (likelihood), determine the impact (impact), the determination of risks, control recommendations and documentation of results. The results of the risk assessment against the academic information system E-University is there are three risks disrupting existing activities in the system. Then from the results of the assessment of risks in the form of recommendations are used to minimize the risks that occur on the system.

Kata kunci:*Assessment, NIST, Risk Management*

Abstrak

Teknologi informasi telah menjadi bagian penting dari kehidupan manusia sehingga dapat mempermudah suatu kegiatan bisnis. Meskipun begitu, penggunaan teknologi informasi tidak lepas dari resiko yang dapat mempengaruhi proses kegiatan tersebut. Adapun tujuan penelitian ini adalah untuk melakukan penilaian resiko terhadap potensi kerentanan dan ancaman yang dapat menyerang sistem informasi akademik E-University sekaligus mempersiapan tindakan antisipasi terhadap hal-hal yang dapat mengganggu sistem. Untuk melakukan penilaian tersebut, study ini menggunakan framework NIST SP 800-30r-1 yang terdiri sembilan tahapan untuk dalam penilaian resiko yaitu karakteristik sistem yang digunakan, indentifikasi ancaman yang menyerang sistem, identifikasi vulnerability, pengendalian sistem, menentukan kemungkinan terjadi (*likelihood*), menentukan dampak (*impact*), penentuan resiko, rekomendasi pengendalian dan dokumentasi hasil. Hasil dari penilaian resiko terhadap sistem informasi akademik E-University adalah terdapat tida resiko yang mengganggu aktifitas yang ada dalam sistem. Kemudian dari hasil penilaian resiko berupa rekomendasi yang digunakan untuk memperkecil resiko yang terjadi pada sistem.

Kata kunci:*NIST, Penilaian Resiko, Risk Management,*

1. PENDAHULUAN

Peran penting teknologi informasi dan komunikasi (TIK) adalah membantu meringankan pekerjaan kantor sehingga lebih cepat dan lebih akurat. Hal ini dapat dilihat dari semakin tergantungnya proses bisnis suatu organisasi di berbagai bidang kegiatan dengan teknologi ini.Bidang pendidikanpun tidak lepas dari penggunaan TIK terutama dalam pelayanan akademik. Secara eksternal, banyak aktifitas pelaporan kegiatan akademik mengharuskan lembaga pendidikan menggunakan TIK. Dukungan teknologi juga dipergunakan untuk mempercepat proses layanan akademik dalan suatu perguruan tinggi. Akibatnya semakin pentingnya peran TIK dalam mendukung kegiatan menimbulkan permasalah tersendiri bila fungsi TIK tersebut terganggu.Pemanfaatan juga TIK perlu untuk memperhatikan resiko yang berpotensi menganggu akibat pengelolaan yang kurang efektif. Pemanfaatan teknologi informasi dapat berjalan dengan efektif jika digunakan dengan baik (Suzanto and Sidharta 2015).

Pemanfaatan TIK yang tidak dimanfaatkan secara baik menimbulkan peluang untuk seseorang melakukan kejahatan dalam teknologi informasi.Pemanfaatan sistem informasi akademik dapat berjalan dengan baik jika dalam penggunaan dan pemanfaatan sistem dapat digunakan secara baik(Cahyaningdyah and Ressany 2012).Kejahatan TIK dapat digolongkan dari yang mengesalkan (*annoying*) sampai dengan sangat berbahaya. Dari yang dapat diatasi sampai yang tidak dapat diatasi yang dapat menimbulkan kehilangan aset terpenting dalam sistem. Untuk mengantisipasi resiko kehilangan aset, maka dibutuhkan sebuah keamanan sistem yang dibuat untuk melindungi teknologi informasi yang ada pada lembaga. Menurut Rahardjo (2002) berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu resiko keamanan yang bersifat fisik *(physical security)*, resiko keamanan yang berhubungan dengan orang (*personel*), resiko keamanan dari data dan media serta teknik komunikasi dan resiko keamanan dalam operasi.

E-University adalah sebuah antarmuka yang menyediakan informasi-informasi seperti jadwal kuliah, matakuliah apa saja yang diambil, nilai persemester, data pengguna serta wadah yang digunakan oleh mahasiswa untuk melakukan ujian *oline* disetiap matakuliah. Dalam pengelolaannya, sistem E-University dikelolah oleh tiga orang yaitu kepala UPT, *programmer* dan staf jaringan yang mempunyai peranan masing-masing didalam sistem.

Terkadang dalam penerapan sistem informasi akademik belum optimal seperti aktifitas dalam penggunaan sistem terhambat karena mendapatkan penyerangan dari penyusup berupa serangan *Ddos*, serangan *phising*, serangan terhadap *port-port* yang digunakan sistem, melakukan *scanning* sistem untuk memperoleh data penting yang ada pada sistem informasi akademik E-University sehingga membuat server menjadi *down*. Seiring berkembangnya teknologi sering kali dimanfaatkan oleh beberapa pihak yang tidak bertanggung jawab yang dapat menyebabkan munculnya ancaman dan resiko dari penggunaan teknologi.Permasalahan keamanan sistem informasi mendapatkan perhatian dari para *stakeholder* dan pengelola sistem informasi ketika sudah terjadi sebuah ancaman yang menimbulkan kerugian pada lembaga. Untuk memperkecil resiko, maka diperlukan penilaian terhadap resiko yang timbul karena kerentanan yang ada dalam sistem. Penilian resiko terhadap sistem merupakan elemen penting dalam menyediakan pelayanan kepada pengguna sistem.Pelayanan akademik yang tepat dan cepat tergantung pada peranan sistem informasi yang didukung oleh teknologi informasi serta SDM (Sumber Daya Manusia) yang mencukupi dan terlatih dalam penggunaan sebuah teknologi informasi.

2. METODOLOGI PENELITAN

2.1 Risk Management Framework

Risk management atau manajemen resiko adalah suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman, suatu rangkaian aktivitas manusia termasuk penilaian resiko, pengembangan strategi untuk mengelolanya dan mitigasi resiko dengan menggunakan pembersayaan/pengelolaan sumberdaya (Hanafi 2014).Tujuan dari manajemen risiko adalah untuk mengenali risiko dalam sebuah proyek dan mengembangkan strategi untuk mengurangi atau bahkan menghindarinya, dilain sisi juga harus dicari cara untuk memaksimalkan peluang yang ada (Wideman 1992).*Framework* adalah kumpulan perintah atau fungsi dasar yang membentuk aturan-aturan tertentu dan saling berinteraksi satu sama lain sehingga dalam pembuatan aplikasi (Wardana and Si 2010).*Framework* yang digunakan oleh penulis adalah *framework* NIST SP 800-30r1 yang tepat digunakan dalam penelitian ini. NIST 800-30r1 adalah dokumen standar yang dikembangkan oleh *National Institute of Standards and Technology* yang mana merupakan kelanjutan dari tanggung jawab hukum dibawah undang-undang *Computer Security Act* tahun 1987 dan *the Information Technology Management Reform Act* tahun 1996 (NIST 2002). Terdapat tiga proses dalam manajemen resiko: *risk assessment, risk mitigation, and evaluation and assessment.Framework* NIST SP 800-30r1 mempunyai struktur dan tahapan proses yang terarah. Metode ini memberikan panduan untuk melakukan proses penilaian resiko langkah demi langkah. Tahapannya terdiri dari *Risk Assessment, Risk Mitigation* dan *Evaluation and Assessment.*

2.2 Teknik Penilaian Resiko

Teknik penilaian resiko menggunakan *framework NIST* SP 800-30r-1. *Framework* NIST SP 800-30r-1 merupakan panduan untuk memproses data yang sangat sensitif. NIST SP 800-30r-1 memiliki kontribusi lebih dalam melakukan penilaian resiko karena memberikan wawasan keamanan informasi yang sifatnya konsisten dan komprehensif bagi pengambilan kebijakan, pemodelan sumber daya yang terstruktur, wawasan keamanan dapat diterima oleh berbagai pengambil resiko, penentuan ancaman dapat diidentifikasi dengan mudah, pengambilan keputusan yang baik untuk setiap resiko yang diselidiki (Andani 2014). Dalam NIST SP 800-30r-1 ini terdapat sembilan langkah untuk melakukan analisa resiko yaitu karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, analisa kontrol, analisa kemungkinan terjadi, analisa dampak, penentuan level resiko dan rekomendasi pengendalian.

2.3 Teknik Pengumpulan Data

Pengumpulan data sangat penting dalam penelitian, karena data tersebut dimaksudkan untuk berkontribusi pada pemahaman kerangka teoretis yang lebih baik (Herdiansyah 2013). Pemilihan informan dengan metode *purposive sampling* bertujuan untuk penelitian yang dilakukan peneliti akan mendapatkan capaian yang baik dan sesuai dengan keinginan informan. Pemilihan informan yang dilakukan peneliti dalam menganalisis *assessment* resiko pada sistem akademik online E-University yaitu memilih sumber data yang benar-benar bertanggung jawab atas sistem tersebut yaitu kepala UPT, *Programmer* dan Staf jaringan yang bertanggung jawab dan terlibat langsung dalam sistem informasi akademik E-University.

2.4 Metode Pennetuan Informan

Pengumpulan data sangat penting dalam penelitian, karena data tersebut dimaksudkan untuk berkontribusi pada pemahaman kerangka teoretis yang lebih baik (Herdiansyah 2013). Menentukan sampel dalam penelitian, terdapat teknik sampling yang digunakan salah satunya adalah teknik purposive sampling. *Purposive sampling* adalah teknik pengambilan sumber dengan pertimbangan tertentu. Misalnya akan melakukan penelitian tentang kualitas suatu makanan, maka sampel yang merupakan sumber data dari penelitian tersebut adalah orang yang ahli dalam makanan. Sampel ini digunakan untuk penelitian kualitatif atau penelitian-penelitian yang tidak melakukan generalisasi (Aryani and Rosinta 2011). Pemilihan informan dengan metode *purposive sampling* bertujuan untuk penelitian yang dilakukan peneliti akan mendapatkan capaian yang baik dan sesuai dengan keinginan informan. Pemilihan informan yang dilakukan peneliti dalam menganalisis *assessment* resiko pada sistem akademik online E-University yaitu memilih sumber data yang benar-benar bertanggung jawab atas sistem tersebut yaitu kepala UPT, *Programmer* dan Staf jaringan yang bertanggung jawab terhadap sistem.

3. HASIL DAN PEMBAHASAN

Untuk melakukan penilaian resiko terhadap sistem informasi akademik E-University ada sembilan tahapan yaitu:

a. Karakteristik Sistem

Karakteristik yang digunakan dalam sistem informasi akademik E-University adalah perangkat keras yang digunakan PC dengan server luar dan sever lokal yang dalah satunya serverbya menggunakan *cloud*. *Software* yang digunakan berupa linux *free* BSD. Jaringan komunikasi yang digunakan adalah sistem komunikasi ekslusif melalui satelit yang memungkinkan pengguna E-University secara *online*. Untuk menjamin sistem yang digunakan aman dalam melakukan transaksi makan digunakan SSL *(Secure Socket Layer)*.

b. Identifikasi Ancaman

Ancaman-ancaman yang mengancam sistem informasi akademik E-University adalah mengubah *plug in* dan *thema* yang ada pada sistem informasi akademik E-University. Melakukan ancaman seperti *sniffing, scanning network, phising, flooding, wireless jamming, Ddos* pada sistem informasi yang bertujuan merusak sistem.

c. Identifikasi Kerentanan (*Vulnerability*)

Identifikasi kerentanan (*Vulnerability*) yang didapat dari hasil wawancara terlihat pada tabel 1.

Tabel 1: Identifikasi Kerentanan (*Vulnerability*)

Jenis Resiko	Kerentanan
Berasal dari dalam Lingkungan	- *Password cracking* untuk melakukan pencurian data pada sistem - Keterlambatan dalam melakukan *updateantivirus* sehingga memungkinkan *malware* masuk kedalam sistem - Kelalaian staf dalam memindahkan sistem - menggunakan *flash drive* yang berisi

Jenis Resiko	Kerentanan
	malware
Berasal dari luar lingkungan	- *Scanning tools*
Bencana alam	- Kebakaran
	- Gempa Bumi

d. Analisis Pengendalian

Hasil dari wawancara terstruktur analisis pengendalian telah tertuang dalam dokumen yang mencakup semua standar-standar dan prosedur-prosedur dalam pengoperasian sistem informasi akademik E-University yaotu dokumen SOP (*Standard Operating Procedure)*

e. Kemungkinan Terjadi (*Likelihood*)

Hasil dari kemungkinan terjadi (*Likelihood*) pada sistem informasi akademik E-University berdasarkan tingkat kemungkinan terjadinya resiko ada tiga yaitu tinggi, sedang dan rendah. Kategori kemungkinan terjadi resiko pada sistem termasuk tinggi apabila sumber ancaman sangat mampu dan pengendalianuntuk mencegah kerentanan yang dilkaukan sudah tidak efektif lagi. Kategori kemungkinan terjadi resiko pada sistem termasuk sedang apabila sumber ancaman mampu dalam menembus pertahanan sistem namun belum sampai pada layer terdalam pada jaringan sehingga dapat menghambat kerentanan. Kategori kemungkinan terjadi resiko pada sistem termasuk rendah apabila sumber ancaman tidak memiliki kemampuan untuk menembus keamanan, setidaknya dapat menghambat namun dapat diatasi. Kemungkinan terjadi resiko pada sistem informasi akademik adalah (1) penyerangan yang dilakukan oleh orang dalam (bisa ditimbulkan dari staf, mahasiswa maupun dosen), (2) terjadi kerusakan atau *disk error* pada penyimpanan data, (3) *plug in* yang terlambat diperbarui.

f. Analisis Dampak (*Impact*)

Berdasarkan analisis hasil resiko yang menggambarkan dampak resiko (*impact*) terhadap sistem informasi akademik E-University terlihat pada tabel 2.

Tabel 2: Dampak Resiko

Jenis Resiko	Dampak	Tingkat Dampak
Penyerangan yang dilakukan oleh orang dalam	- Tidak dapak masuk kedalam sistem - Pencurian data pengguna	Tinggi
Disk Error	- Tidak dapat melakukan proses penyimpanan data pada hardisk	Sedang
Plug in yang terlambat diperbarui	- Kerusakan kecil pada ditampilan interface sistem	Rendah

g. Risk Determination

Risk determination memperlihatkan jenis resiko yang menyerang sistem informasi akademik E-University dari yang tinggi sampai ke resiko yang rendah yang akan terlihat pada tabel 3. Pada tabel 3 terlihat jenis resiko yang memiliki tingkat atau level resiko tinggi pada jenis resiko penyerangan yang dilakukan oleh orang dalam. Level resiko sedang pada jenis resiko *disk error* atau kerusakan pada penyimpanan data dan terakhir adalah *plug in* yang terlambat diperbarui yang memiliki level resiko rendah.

Tabel 3:*Risk Determination*

Jenis Resiko	Nilai Kemungkinan Terjadi	Nilai Dampak	Nilai Resiko	Level Resiko
Penyerangan yang dilakukan oleh orang dalam	1,0	100	100	Tinggi
Disk Error	0,5	100	50	Sedang
Plug in yang terlambat diperbarui	0,1	100	10	Rendah

h. Rekomendasi Pengendalian

Dari tingkat resiko tersebut dapatlah rekomendasi pengendalian yang digunakan untuk membuat prosedur untuk penanganan terhadap ancaman yang terjadi. Dari hasil penilaian maka direkomendasikan beberapa kontrol yang dapat dilakukan terhadap resiko yang terlihat pada tabel 4.

Tabel 4: Rekomendasi Pengendalian

Jenis Ancaman	Tingkat Ancaman		Rekomendasi Pengendalian
Penyerangan yang dilakukan oleh orang dalam	Tinggi	-	Memperkokoh *firewall* yang digunakan oleh sisem informasi akademik E-University, Tidak menampilkan jenis *web* editor apa yang digunakan untuk membangun sistem informasi akademik E-University
Disk Error	Sedang	-	*Backup data*
Plug in yang terlambat diperbarui	Rendah	-	Memberikan pelatihan terhadap penggunaan sistem informasi akademik E-university

i. Dokumen Hasil

Dari hasil penilaian resiko teknologi pada implementasi sistem informasi akademik E-University maka dibuatlah dokumen penanganan terhadap resiko yang mengancam sistem informasi akademik E-University. Dokumen ini berisi tentang tata cara penanganan resiko-resiko yang menyerang sistem informasi akademik.

4. KESIMPULAN

Dalam proses penilian resiko, penulis menggunakan tahapan resiko yang telah disediakan oleh *framework* NIST SP 800-30r-1 yang terdiri dari karakteristik sistem, mengidentifikasi ancaman, kontrol analisis, kemungkinan terjadi (*likelihood*), dampak (*impact*), level resiko *(risk determination*), rekomendasi resiko dan terakhir rekomendasi hasil. Diantara jenis ancaman ini terdapat 3 tingkat resiko setelah dilakukan penilaian. Resiko yang muncul adalah resiko yang dilakukan oleh orang dalam serta kegagalan infrastruktur. Resiko dinilai mempunyai resiko tinggi karena penyerangan yang dilakukan terhadap sistem berasal dari orang dalam seperti staf, dosen atau mahasiswa. Resiko ini dinilai mempunyai resiko sedang karena tempat penyimpanan data rusak yang membuat aktifitas dalam sistem menjadi terganggu. Serta resiko ini dinilai mempunyai resiko rendah karena*plug in* yang terlambat diperbarui sehingga penyusup dapat mengubah beberapa menu pada tampilan *interface*.

Referensi

Andani, M. (2014). Manajemen Risiko Keamanan Aplikasi Sistem Informasi Laporan Harian Pks & Ppko Online Pada Ptpn V Menggunakan Metode Nist Sp 800-30, *Universitas Islam Negeri Sultan Syarif Kasim Riau.*

Aryani, D. and F. Rosinta (2011). Pengaruh kualitas layanan terhadap kepuasan pelanggan dalam membentuk loyalitas pelanggan. *BISNIS & BIROKRASI: Jurnal Ilmu Administrasi dan Organisasi.*

Cahyaningdyah, D. And Y.D. Ressany (2012), Pengaruh Kebijakan Manajemen Keuangan Terhadap Nilai Peusahaan, *Jurnal Dinamika Manajemen*.

Herdiansyah, H. (2013). *Wawancara, observasi, dan focus groups: Sebagai instrumen penggalian data kualitatif*. Jakarta: PT. Raja Grafindo Persada.

Mellisa, M. And F. A. Andono (2013). *Penerapan Enterprise Risk Management dalam Rangka Meningkatkan Efektifitas Kegiatan Operasional CV. Anugerah Berkat Calindo Jaya.*

NIST (2002). Sp 800-30. risk management guide for information technology systems. *Recomendation of National Institute of Standards and Technology Special Publication 800-30r-1*.Rahardjo, B. (2002). Keamanan Sistem Informasi Berbasis Internet. *PT Insan Infonesia–Bandung & PT INDOCISC–Jakarta.*

Suzanto, B. and I. Sidharta (2015). Pengukuran End-User Computing Satisfaction Atas Penggunaan Sistem Informasi Akademik. *Jurnal Ekonomi, Bisnis & Entrepreneurship*.

Wardana, S. H. and M. Si (2010). *Menjadi Master PHP dengan Framework Codeigniter, Elex Media Komputindo,* www.scholar.google.co.id, diakses: 18 Maret 2018.

Wideman, R. M. (1992). Project and program risk management: a guide to managing project risks and opportunities, *University of Maribor, Faculty of Business and Economics.*