Analisis Manajemen Risiko Sistem Informasi Pengelolaan Data English Proficiency Test (EPT) dan Portal Informasi di UPT Bahasa Universitas Lampung Menggunakan Metode ISO 31000

[1]Monica, [2]Didik Kurniawan & [3]Rizky Prabowo

[1,2,3] Jurusan Ilmu Komputer FMIPA Universitas Lampung
Jalan Prof. Sumantri Brojonegoro No. 1 Bandar Lampung 35145

[1]monicamonik77@gmail.com, [2]didikunila@gmail.com, [3]rizky.prabowo@fmipa.unila.ac.id,

Abstract —UPT Language University of Lampung (Unila) is one of the Technical Services Unit (UPT) that utilizes information systems to support effectiveness and efficiency in its implementation in the field. The purpose of this study is to analyze the process of information system risk management at the Unila Language UPT using ISO 31000 and produce recommendations for work units about effective control measures and appropriate treatment for the risks faced. Information system risk management at UPT Language Unila is implemented to anticipate the source of risk threats by means of communication and consultation, setting the context (scope), risk assessment, monitoring and review, and handling. The results of this risk management research are, there are 15 possible risks. These risks are classified into 3 risk categories including personnel risk, system and infrastructure risks, and incidental risks. The level of risk is divided into 5 namely, very high risk, high risk, moderate risk, low risk, and very low risk.

Keywords: Risk Management, Information Systems, ISO 31000, UPT Language Unila

5. Pendahuluan

UPT Bahasa Universitas Lampung (Unila) merupakan salah satu Unit Pelayanan Teknis (UPT) yang membantu universitas dalam mengimplementasikan program dan kegiatan yang menunjang pembelajaran dan layanan kebahasaan. Dalam meningkatkan pelayanannya, UPT Bahasa memanfaatkan sistem informasi yang dapat menunjang efektifitas dan efisiensi dalam pengimplementasiannya dilapangan.

Dalam pengimplementasiannya, terdapat risiko yang ditimbulkan pada tahapan-tahapan proses bisnisnya. Penggunaan sistem informasi harus diiringi dengan pengelolaan informasi yang tepat dan sesuai sehingga dapat meminimalisir risiko-risiko yang mungkin terjadi didalam proses bisnisnya.

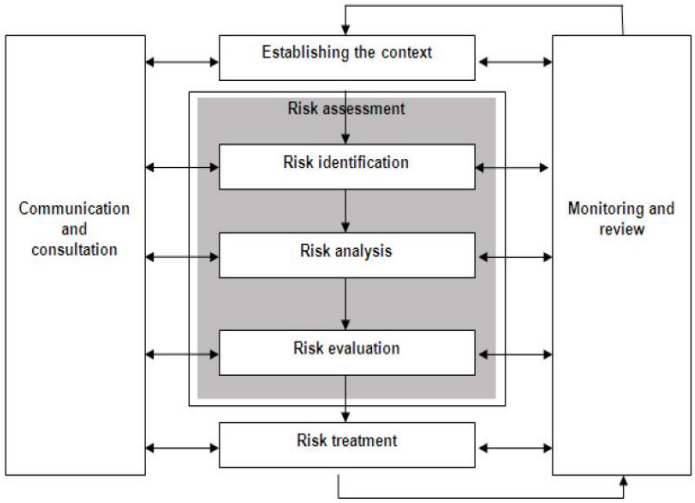
Proses menganalisa serta memperkirakan timbulnya suatu risiko dalam suatu kegiatan disebut sebagai manajemen risiko [1]. Dengan adanya manajemen risiko dapat mengetahui risiko apa yang dapat merugikan bagi pihak UPT maupun pengguna.

Dalam penelitian ini dapat menggunakan metode ISO 31000. Standar ISO 31000 memiliki perspektif yang jauh lebih luas yaitu dapat diterapkan dalam berbagai lingkup maupun kegiatan, dan lebih konseptual dibandingkan dengan standar lainnya [2]. Untuk mengetahui proses penerapan manajemen risiko sistem informasi UPT Bahasa tersebut, diperlukan penelitian tentang sejauh mana penerapan manajemen risiko sistem informasi UPT Bahasa dalam menilai sumber

ancaman dan kerentanan, menganalisis, mengurangi, serta mengevaluasi risiko terhadap aset informasi UPT Bahasa di Unila.

6. Proses Manajemen Risiko

Proses manajemen risiko menggunakan metode ISO 31000 meliputi identifikasi risiko, analisis risiko dan evaluasi risiko.



Gambar 1. Proses Manajemen Risiko [3]

Adapun tahap yang dilakukan yaitu:

a. Identifikasi Risiko

Tahapan identifikasi risiko adalah sebagai berikut:

1. Identifikasi risiko sistem yaitu dengan mengumpulkan data mengenai perangkat keras, perangkat lunak, keamanan sistem, dan fungsi dari sistem. Hal ini dilakukan untuk mengetahui batasan-batasan apa saja pada sistem informasi di UPT Bahasa.
2. Identifikasi risiko personil yaitu dengan mengumpulkan data mengenai ancaman sumber risiko pada sistem serta bentuk ancaman dari setiap sumber risiko tersebut yang berasal dari tindak kejahatan yang diakibatkan oleh manusia.
3. Identifikasi risiko insidental yaitu dengan mengumpulkan data mengenai risiko-risiko apa saja yang diakibatkan oleh faktor alam atau lingkungan yang dapat menghabat jalannya kegiatan di UPT Bahasa.

b. Analisis Risiko

Tahapan analisis risiko adalah sebagai berikut:

1. Menentukan status risiko untuk mendapatkan peringkat *likehood* yang mengindikasikan probabilitas bahwa sumber ancaman berpotensi dapat melakukan ancaman.

2. Analisis dampak yaitu dengan menentukan dampak buruk yang diakibatkan sebuah ancaman yang berhasil dilakukan.

c. Evaluasi Risiko

Tahapan evaluasi resiko adalah dengan menentukan risiko dinilai dari pengumpulan data pada tahap sebelumnya seperti *likehood* serta dampak yang dihasilkan dari setiap risiko. Sehingga pada tahap ini akan menghasilkan peringkat risiko yang terjadi pada sistem informasi di UPT Bahasa.

7. Pembahasan

a. Identifikasi

Berdasarkan hasil observasi dan wawancara pada pihak UPT Bahasa, terdapat 15 kemungkinan terjadinya risiko. Risiko tersebut digolongkan menjadi 3 kategori risiko antara lain risiko personil, risiko sistem dan infrastruktur, dan risiko insidental.

b. Analisis Risiko

Analisis risiko pada penelitian ini dilakukan dengan cara memberikan kuisioner kepada pihak UPT Bahasa untuk mengetahui besaran kemungkinan terjadinya risiko dan dampak yang ditimbulkan akibat risiko tersebut. Formula untuk menghitung status risiko adalah: *Level* Risiko = Probabilitas x Dampak.

c. Evaluasi Risiko

Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas risiko-risiko tersebut. Untuk menentukan peringkat risiko, diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Berikut ini adalah tabel peta risiko sistem CAT-EPT dan portal informasi yang dapat dilihat pada Gambar 2 di bawah ini:

Matriks Analisis Risiko			Level Dampak				
			1	2	3	4	5
			Sangat Kecil	Kecil	Menengah	Besar	Sangat Tinggi
Level Kemungkinan	5	Hampir Pasti	A6, B4	A4			
	4	Sering		B1, C3		B3	
	3	Kadang	B5	A5			
	2	Jarang				C2	
	1	Hampir Tidak		A1, B6	A3, B2	A2, C1	

Gambar 2. Peta Risiko

Menetapkan *level* risiko yaitu batasan besaran kuantitatif *level* kemungkinan terjadinya risiko dan *level* dampak risiko yang dapat diterima, sebagaimana dituangkan pada kriteria risiko. *Level* sangat tinggi (5) disimbolkan dengan warna merah, *level* tinggi (4) disimbolkan dengan warna orange, *level* sedang (3) disimbolkan dengan warna kuning, *level* rendah (2) disimbolkan dengan warna hijau, dan *level* sangat rendah (1) disimbolkan dengan warna biru. Berikut ini merupakan tabel *level* risiko yang dapat di lihat pada Tabel 1 di bawah ini:

Tabel 1. Level Risiko

Level Risiko	Besaran	Simbol
Sangat Tinggi (5)	15	
Tinggi (4)	10	
Sedang (3)	5	
Rendah (2)	3	
Sangat Rendah (1)	1	

d. Rekomendasi Penanganan

Perlakuan risiko meliputi upaya untuk menyeleksi pilihan-pilihan yang dapat mengurangi atau meniadakan dampak serta kemungkinan terjadinya risiko. Perlakuan terhadap suatu risiko dapat berupa salah satu dari empat perlakuan sebagai berikut:

1. Menghindari risiko (*risk avoidance*): dengan melakukan penanganan risiko dengan mengubah atau menghilangkan sasaran atau kegiatan untuk menghilangkan risiko tersebut.
2. Mengalihkan risiko (*risk sharing/risk transfer*): manajemen mengelola risiko lain dengan bersekutu dengan pihak lain melalui *joint venture* dan *joint financing* dalam rangka menanggung risiko tersebut bersama-sama.
3. Mengurangi atau mitigasi (*mitigation*): melakukan perlakuan risiko untuk mengurangi kemungkinan timbulnya risiko, atau mengurangi dampak risiko bila terjadi, atau mengurangi keduanya. Mengelola risiko dengan membuat prosedur dan pengawasan internal, pelatihan atau sosialisasi internal.
4. Menerima risiko (*risk acceptance*): manajemen menerima risiko tersebut sebagaimana adanya karena ada ketentuan seperti: sudah diamanatkan oleh undang-undang atau karena faktor alam.

Berikut ini adalah tabel identifikasi, analisis, evaluasi dan penanganan risiko yang dapat dilihat pada Tabel 1 di bawah ini:

Tabel 2. Identifikasi, Analisis, Evaluasi dan Rekomendasi Penanganan risiko

Jenis	Kode	Identifikasi	Analisa *Level*	Evaluasi	Rekomendasi
Personil	A1	Pencurian Perangkat	Sangat Rendah	Pengawasan yang kurang ketat dapat menimbulkan pencurian perangkat. Hal ini terjadi apabila ada peserta yang mencuri fasilitas di lab.	Dengan mengumpulkan tas peserta diruangan, tidak diperkenankan membawa kotak pensil atau sejenisnya, memeriksa saat tes selesai, memasang CCTV dan *sensor alarm security*.
	A2	Kebocoran data internal	Rendah	Pengawasan yang kurang ketat	Dengan melakukan pengawasan yang ketat

Jenis	Kode	Identifikasi	Analisa *Level*	Evaluasi	Rekomendasi
		UPT Bahasa (soal)		terhadap peserta tes dapat menimbulkan kebocoran soal. Hal itu bisa terjadi apabila peserta mengambil gambar atau merekam soal-soal saat tes menggunakan *handphone*.	saat tes. Seperti melarang membawa *handphone*, kamera dan alat perekam lainnya saat melakukan tes, dan memantau pelaksaan tes pada CCTV.
	A3	Kelalaian dalam memasukan data (ada 1-2 soal yang salah)	Rendah	Saat meng*input* bank soal, sering terjadi kesalahan penulisan dalam soal.	Dengan memeriksa kembali pada saat bank soal di *input* atau dengan membuat SOP peng-*input*-an bank soal. Mencatat soal yang salah dan soal yang salah dihitung bonus pada saat pengelolaan data, supaya tidak merugikan peserta yang tes.
	A4	Penyalahgunaan hak akses/*User ID* (peserta)	Tinggi	Sering terjadi kecurangan yang dilakukan oleh peserta saat melakukan tes, yaitu dengan menggunakan joki saat melaksanakan tes.	Dengan memasang sistem pengenalan wajah untuk mengidentifikasi peserta tes.
	A5	*Human error* (nilai)	Sedang	Kesalahan dalam menampilkan hasil nilai.	Melakukan pelatihan pada pegawai, membuat pembatasan hak akses sesuai dengan tingkat kepentingannya, melakukan pengawasan secara internal terhadap apa yang dikerjakan.
	A6	Data *double*	Sedang	Peserta bisa mendaftar beberapa kali dalam satu waktu dan tidak bisa dihapus.	Dengan melakukan perbaikan terhadap kekurangan sistem informasi seperti peserta tidak bisa tidak mendaftar sebelum proses verikasi selesai.
sistem dan infrastruktur	B1	*Vandalism* (merusak fasilitas seperti meja, kursi, dan	Rendah	Menulis-nulis pada meja dengan pena.	Dengan memberi peringatan kepada peserta sebelum tes dimulai untuk tidak merusak dan menjaga fasilitas yang

Jenis	Kode	Identifikasi	Analisa *Level*	Evaluasi	Rekomendasi
		perangkat komputer)			diberikan sebelum tes dimulai. Memberi sanksi kepada peserta yang merusak fasilitas seperti, membersihkan bekas coretan, dan mengganti fasilitas yang dirusak.
	B2	*Over heat*	Rendah	Terlalu lama digunakan sehingga membuat perangkat keras menjadi panas.	Dengan memasang pendingin, arus listrik stabil, ruangan bersuhu normal.
	B3	Koneksi yang tiba-tiba *offline*	Sangat Tinggi	Terjadi karena adanya gangguan jaringan seperti *server down*, jaringan terputus, mati lampu, dan lain-lain.	Melaporkan permasalahan ke pihak UPT TIK sesuai dengan SOP. Menyediakan server cadangan yang diletakkan di UPT Bahasa, program aplikasi diinstal pada server LAN yang terdistribusi ke setiap *client* (tidak terkoneksi ke server pusat).
	B4	Sistem *error*	Rendah	*Over load*, *bandwith terbatas*, kesalahan *coding*, virus, atau kesalahan konfigurasi.	Dengan mengajukan penambahan *bandwidth*, melakukan pembaharuan sistem, dan melakukan *update antivirus*.
	B5	*Over load*	Rendah	Terlalu banyak yang ingin tes pada momen tertentu seperti: sebelum pendaftaran wisuda, pembukaan BUMN dan lain-lain. Jumlah PC yang tersedia hanya 54.	Dengan membagi kuota pendaftar seperti: dalam 1 minggu terdapat 3 sesi. Jumlah fakultas di Unila ada 8 dan jumlah jurusan ada 63, sehingga sesi pertama 3 fakultas, sesi kedua 3 fakultas, dan sesi ketiga 2 fakultas.
	B6	*Over capacity*	Sangat Rendah	Tipe data untuk id pada jadwal TINYINT. Kapasitasnya terlalu kecil.	Melakukan *modify* pada *database*, dengan memperbaharui tipe data yang sesuai yang dapat menampung banyaknya data yang masuk setiap harinya.
Insidental	C1	Kebakaran	Rendah	Aliran atau ketengangan listrik, hubungan arus pendek pada	Dengan tidak melakukan aktifitas yang dapat memicu risiko tersebut. Semua peralatan harus dipastikan

Jenis	Kode	Identifikasi	Analisa *Level*	Evaluasi	Rekomendasi
				peralatan elektronik dan lain-lain.	pemasangannnya dengan benar dan perawatan secara rutin. Pastikan karyawan yang menangani peralatan ini telah menerima pelatihan yang tepat, dan tersedia instruksi yang jelas. Serta menyediakan alat pemadam kebakaran.
	C2	Bencana Alam	Sedang	Peristiwa alam seperti hujan, badai dan petir.	Menempatkan *data center* pada tempat yang strategis, artinya terbebas dari ancaman bencana alam seperti gempa, banjir, dan petir. Memasang pengaman anti petir pada *data center*, alat ini bisa mencegah kerusakan pada *data center* yang diakibatkan oleh petir.
	C3	Mati Listrik	Sedang	Pemadaman listrik dalam waktu lebih dari 4 jam atau terjadi pada saat tes berlangsung	Dengan menyediakan genset dan UPS (*Uninterruptible Power Supply*) sebagai alat *back up* listrik ketika PC kehilangan energi dari sumber utamanya.

8. **Kesimpulan**

1. Dengan menggunakan ISO 31000 terlihat nilai risiko dengan lima tingkatan yaitu sangat redah, rendah, sedang, tinggi dan sangat tinggi.
2. Hasil dari identifikasi risiko didapat 15 sumber ancaman pada sistem informasi UPT Bahasa Universitas Lampung. Risiko tersebut digolongkan menjadi 3 kategori risiko yaitu risiko personil, risiko sistem dan infrastruktur, dan risiko insidental.
3. Hasil analisis dan evaluasi risiko terdapat 1 risiko yang bernilai sangat tinggi yaitu (koneksi tiba-tiba *offline*), 1 risiko yang bernilai tinggi yaitu (penyalahgunaan hak akses), 4 risiko bernilai sedang yaitu (*human error*, data *double*, bencana alam, mati listrik), dan 7 risiko bernilai rendah yaitu (kebocoran data soal, kelalaian dalam memasukkan data, *vandalism*, *overload*, *over heat*, sistem *error*, kebakaran) dan 2 risiko yang bernilai sangat rendah yaitu (pencurian perangkat dan *over capacity*).
4. Penanganan risiko yang diterapkan berupa menghindari risiko (*risk avoidance*), mengalihkan risiko (*risk sharing/risk transfer*), mengurangi atau mitigasi (*mitigation*) dan menerima risiko (*risk acceptance*).

DaftarPustaka

[1] Susilo. (2017). Analisa Tingkat Resiko Tata Kelola Teknologi Informasi Perguruan Tinggi Menggunakan Model Framework National Institute of Standards & Technology (NIST) Special Publication 800-30 dan IT General Control Questionnaire (ITGCQ). *Journal Industrial Servicess Vol. 3c No. 1 Oktober 2017*, 240.

[2] Susilo, L. J., dan Kaho, R. V. (2018). *Manajemen Risiko Berbasis ISO 31000: untuk Industri Nonperbankan. Edisi Revisi*. Jakarta: PPM.

[3] ISO. (2009). ISO 31000:2009 Risk Management – Principles and Guidelines. Switzerland: International Organization for Standarization.