Analisa Risiko Teknologi Informasi Berbasis ISO 31000/31010 Studi Kasus: Lembaga Penelitian Perguruan Tinggi

Selvi Amriani
Program Magister Layanan Teknologi Informasi
Institut Teknologi Bandung
email: selvi.amriani@gmail.com

Abstract

Information system and information technology is an important component in organizing a research service unit in higher education institution nowadays. The role of information technology is clearly important in performing a qualified, accountable and accurate service. The goal of this research is to analyze risks that threaten infrastructure and services of information technology in university research service unit. This research is using international standard that is ISO 31000 and ISO 31010 as a framework to identify and analyze information technology risk. The result of this research is an information technology risk catalogue which consists of risk lists and factors that contribute or trigger a certain events that cause an information technology in university research unit.

Keywords: information technology risk, ISO 3100, research service unit

I. Pendahuluan

Seiring dengan meningkatnya volume kegiatan penelitian yang dilaksanakan oleh staf dosen di perguruan tinggi, teknologi informasi merupakan sarana pendukung yang mutlak dibutuhkan untuk meningkatkan kualitas dan akuntabilitas pelayanan dalam pelaksanaan proses bisnis di lembaga penelitian. Seperti hal nya risiko yang mengancam pengelolaan lembaga secara keseluruhan, implementasi sistem dan teknologi informasi di lembaga penelitian perguruan tinggi juga dihadapkan pada risiko berupa ancaman dari berbagai sumber.

Tujuan dan sasaran implementasi teknologi informasi dalam pelaksaan proses bisnis di lembaga penelitian perguruan tinggi secara umum dapat didefinisikan sebagai berikut:

1. Mewujudkan transparansi dan akuntabilitas proses keuangan
2. Mewujudkan transparansi pengadaan barang dan jasa
3. Meningkatkan kualitas pelayanan administrasi pengusulan kegiatan penelitian
4. Memperbaiki mekanisme diseminasi informasi kegiatan penelitian
5. Meningkatkan kualitas layanan penerbitan jurnal ilmiah

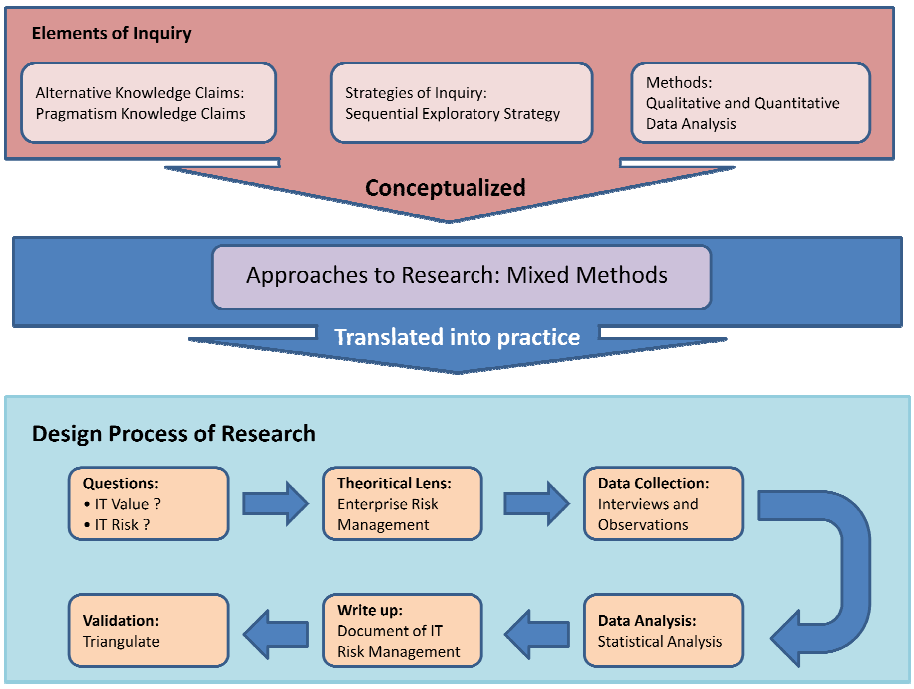
Oleh karena itu, analisa risiko yang berkaitan dengan implementasi teknologi informasi dalam pelaksanaan proses bisnis di lembaga penelitian perguruan tinggi merupakan sesuatu yang sangat penting. Analisa yang menyeluruh terhadap risiko-risiko teknologi informasi dapat dijadikan landasan untuk merumuskan kebijakan dalam rangka mencegah kegagalan layanan teknologi informasi dalam proses bisnis di lembaga penelitian perguruan tinggi.

II. Metodologi

Dalam rancang metodologi penelitian analisa risiko ini, terdapat tiga elemen dari yang diperhatikan yaitu [Cress03]:

1. Asusmsi filosofis (*Philosophical assumptions*) mengenai *knowledge claims*;
2. Prosedur penelitian secara umum (*strategy of inquiry*);
3. Detail prosedur mengenai pengumpulan, pengolahan, dan analisa data (*methods*).

Ketiga elemen penelitian di atas, dikombinasikan untuk membentuk sebuah pendekatan dalam penelitian (*approaches to research*). Kemudian pendekatan penelitian tersebut diterjemahkan ke dalam proses dalam desain penelitian (*design processes of research*). Kombinasi elemen penelitian (*elements of inquiry*) untuk membentuk pendekatan penelitian (*approaches to research*) dan terjemahannya ke dalam proses penelitian (*design processes of research*) dapat dilihat pada Gambar 1 di bawah ini.

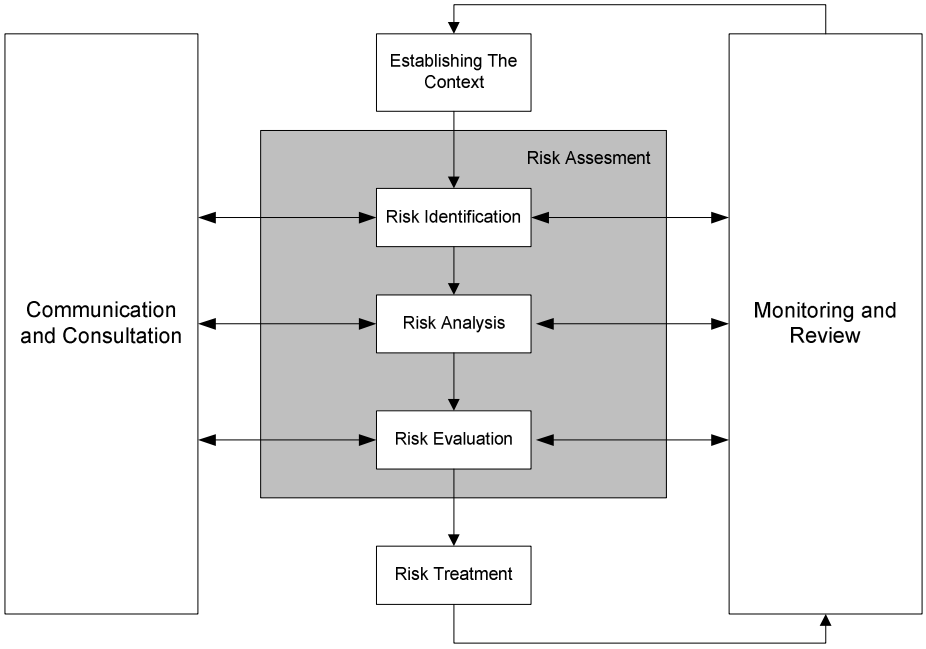


Gambar 1. Metodologi Penelitian Analisa Risiko Teknologi Informasi

III. Tahapan Analisis Risiko Teknologi Informasi

Sim Segal (2011) menguraikan bahwa terdapat tiga aspek dari risiko, yaitu ketidakpastian (*uncertainty*), perubahan (*upside volatility*), dan kesenjangan dari apa yang diharapkan (*deviation from expected*)[Segal11]. Salah satu cara memandang risiko adalah bahwa risiko merupakan kejadian yang peluang terjadinya kurang dari 100 persen. Artinya tidak ada risiko yang pasti terjadi.

International Organization for Standardization (ISO) dalam dokumen International Standard ISO 31000 menetapkan tahapan-tahapan standard dalam proses manajemen risiko sebagaimana diperlihatkan pada Gambar 2 di bawah ini.



Gambar 2. Risk management process [ISO31000]

III.1. Penentuan Konteks

Penentuan konteks dalam proses manajemen risiko adalah proses penentuan tujuan dan sasaran organisasi, pendefinisan parameter internal dan eksternal yang harus dipertimbangkan dalam pengelolaan risiko, serta penentuan cakupan dan kriteria risiko yang akan dijadikan acuan dalam pengelolaan risiko.

Dalam proses manajemen risiko teknologi informasi, konteks eskternal didefinisikan sebagai kondisi atau lingkungan eksternal organisasi teknologi informasi yang berpengaruh terhadap proses manajemen risiko. Konteks eksternal bisa berasal dari luar organisasi TI atau dari luar organisasi induk. Sedangkan konteks internal adalah lingkungan internal organisasi teknologi informasi.

Beberapa konteks eksternal yang mempengaruhi pengelolaan risiko teknologi informasi di lembaga penelitian perguruan tinggi diantaranya adalah:
1. Visi dan Misi Perguruan Tinggi
2. Kebijakan Penelitian Perguruan Tinggi
3. Program dan Sasaran Utama Perguruan Tinggi
4. Rencana Strategis

Beberapa konteks internal dalam pengelolaan risiko teknologi informasi di lembaga penelitian perguruan tinggi diantaranya adalah:

1. Program Pengembangan Sumberdaya Teknologi Informasi
2. Kebijakan pengelolaan SDM TI
3. Kebijakan dan Aturan Tatakelola Teknologi Informasi

Selain konteks eksternal dan internal, perlu ditentukan juga konteks manajemen risiko itu sendiri. Menentukan konteks manajemen risiko adalah menentukan tujuan, sasaran, aktivitas/proses, dan bagian dari organisasi yang berkaitan dengan pengelolaan risiko. Memahami risiko, atau lebih tepatnya lagi, memahami ancaman terhadap sistem dan teknologi informasi memungkinkan sebuah organisasi untuk melindungi sistem dan menyelaraskan nilai dari sistem tersebut dengan tujuan organisasi secara umum. Proses manajemen risiko harus terintegrasi dan berperan untuk pencapaian sasaran organisasi secara keseluruhan. Di lain pihak, sasaran organisasi juga dijabarkan menjadi berbagai sasaran fungsi, unit kerja, dan proyek.

Oleh karena itu, proses manajemen risiko juga harus memastikan bahwa sasaran-sasaran tersebut tercapai. Atas dasar pengertian inilah maka harus dibangun konteks proses manajemen risiko[SUSILO10].

III.2. Kriteria Risiko Teknologi Informasi

Krtieria risiko teknologi informasi ditentukan dengan mempertimbangkan dua aspek yaitu kemungkinan terjadinya risiko dan dampak yang diakibatkan oleh kejadian tersebut.

Panduan umum untuk menentukan besar angka kemungkinan adalah[Susilo10]:

1. Bila tidak ada atau sedikit sekali data yang tersedia, maka dapat digunakan pendekatan *subjective probability, uniform distribution probability,* atau *probability matrix*.
2. Bila terdapat data yang cukup banyak di masa lalu mengenai risiko-risiko yang telah terjadi, bisa dibuat model matematika dan pola distribusinya.

Berikut ini adalah contoh kriteria risiko teknologi informasi yang dapat dijadikan acuan dalam menganalisa risiko implementasi teknologi informasi di lembaga penelitian perguruan tinggi.

Tabel 1 Kriteria Dampak Risiko Teknologi Informasi

	Confidentiality	***Integrity***	***Availability***
Rendah	Hilangnya kerahasiaan yang mengakibatkan dampak yang tidak signifikan	Hilangnya integritas yang mengakibatkan dampak yang tidak signifikan	Tidak tersedianya sistem dan teknologi informasi yang mengakibatkan dampak yang tidak signifikan
Menengah	Hilangnya kerahasiaan yang mengakibatkan dampak signifikan	Hilangnya integritas yang mengakibatkan dampak signifikan	Tidak tersedianya sistem dan teknologi informasi yang mengakibatkan dampak signifikan
Tinggi	Hilangnya kerahasiaan yang mengakibatkan dampak yang sangat siginifikan	Hilangnya integritas yang mengakibatkan dampak yang sangat siginifikan	Tidak tersedianya sistem dan teknologi informasi yang mengakibatkan dampak yang sangat siginifikan

Tabel 2 Peringkat Dampak Risiko Teknologi Informasi

Peringkat Dampak	Dampak terdahap Pelaksanaan Proses Bisnis LPPM ITB	Kerugian Finansial/Dampak terhadap Aset LPPM
Dampak Tidak Signifikan	Pelaksananan Proses Bisnis LPPM ITB tidak terganggu	Kerugian finansial kurang dari 25 juta rupiah
Dampak Signifikan	Gangguan operasional terhadap pelaksanaan proses Bisnis LPPM ITB	Kerugian finansial antara 25 juta sampai dengan 50 rupiah
Dampak Sangat Signifikan	Pelaksananan Proses Bisnis LPPM ITB terhenti	Kerugian finansial lebih dari 50 juta rupiah

Tabel 3 Kriteria Kemungkinan Kejadian Risiko Teknologi Informasi

Peringkat Kemungkinan	Definsi
Rendah	Kemungkinan kejadian risiko adalah 0-25% dalam periode satu tahun
Menengah	Kemungkinan kejadian risiko adalah 26-75% dalam periode satu tahun
Tinggi	Kemungkinan kejadian risiko adalah 76-100% dalam periode satu tahun

IV. Identifikasi Risiko Teknologi Informasi

Dalam manajemen resiko teknologi informasi, terdapat beberapa jenis sumber ancaman (*threat*) terhadap sistem dan teknologi informasi, diataranya [SANS07]:

1. *Accidental disclosure*
   Penyalahgunaan mandat yang diberikan atau membeberkan secara sengaja suatu informasi rahasia, perorangan, atau terklasifikasi.
2. *Act of Nature*
   Ancaman yang disebabkan oleh alam (gempa bumi, tornado, badai) yang menyebabkan kegagalan sistem, kerusakan, dan ancaman lainnya.
3. *Alteration of Software*
   Upaya untuk menambahkan, memodifikasi, menghapus, suatu sistem (aplikasi, sistem operasi), yang mengancam integritas data, ketersediaan, serta sumberdaya yang dikontrol oleh sistem, serta kerusakan sistem. Termasuk di dalamnya trojan, virus, dan malicious code.
4. *Bandwith Usage*
   Penggunaan komunikasi bandwith untuk tujuan tertentu diluar kepentingan organisasi.
5. *Electrical Interference/Disruption*
   Interferensi/fluktuasi yang menyebabkan kegagalan sistem, baik dengan otoritas user maupun modifikasi data.
6. *Intentional Alteration of Data*
   Upaya untuk memodifikasi, menambah, memasukkan sebuah data, baik menggunakan akun terotentikasi maupun tidak, yang menyebabkan kerusakan data (penyimpanan, produksi, proses, dan kontrol).
7. *System Configuration Error (Accidental)*

Kesalahan konfigurasi yang tidak disengaja saat melakukan proses upgrade sistem, software, hardware, peralatan komunikasi operasional.

8. *Telecommunication Malfunction/Interruption*
   Kegagalan sistem pada media komunikasi, unit, komponen, yang menyebabkan terjadinya interupsi pada transfer data melalui telekomunikasi diantara komputer, distribusi pemrosesan secara remote,dan lainnya.

Identifikasi risiko dilakukan menggunakan teknik yang telah ditetapkan oleh *International Organization for Standardization* dalam dokumen ISO 31010 dengan mempertimbangkan sumber ancaman terhadap sistem dan teknologi informasi.

V.1. Teknik Identifikasi Risiko

International Organization for Standardization dalam dokumen ISO 31010 menyajikan 31 alternatif teknik untuk melakukan identifikasi risiko, analisa risiko dan evaluasi risiko. Teknik identifikasi risiko teknologi informasi di lembaga penelitian perguruan tinggi ditentukan dengan mempertimbangkan beberapa alasan berikut ini:

1. Teknik identifikasi risiko harus dapat dijustifikasi dan harus sesuai dengan situasi atau karakteristik organisasi;
2. Teknik identifikasi risiko harus dapat memberikan hasil dalam bentuk yang menyajikan pemahaman yang lebih mendalam tentang sifat dari risiko dan bagaimana risiko tersebut dapat diatasi;
3. Teknik identifikasi risiko harus bersifat *traceable, repeatable and verifiable*.

Dalam penelitian ini, teknik identifikasi yang digunakan untuk melakukan identifikasi risiko teknologi informasi di lembaga penelitian perguruan tinggi adalah ***Preliminary hazard analysis*** **(PHA)**.

Data input yang digunakan untuk melakukan identifikasi dengan teknik diataranya *Preliminary hazard analysis* (PHA) adalah:

1. Informasi mengenai sistem dan teknologi yang akan dinilai.
2. Detail informasi yang tersedia dan relevan mengenai desain dan sistem teknologi informasi yang akan dinilai.

V.2. Hasil Identifikasi Risiko

Hasil identifikasi risiko teknologi informasi dengan menggunakan teknik *Preliminary Hazard Analysis* dapat dilihat pada tabel 4 yaitu katalog risiko teknologi informasi di lembaga penelitian perguruan tinggi.

Tabel 4 Katalog Risiko Teknologi Informasi

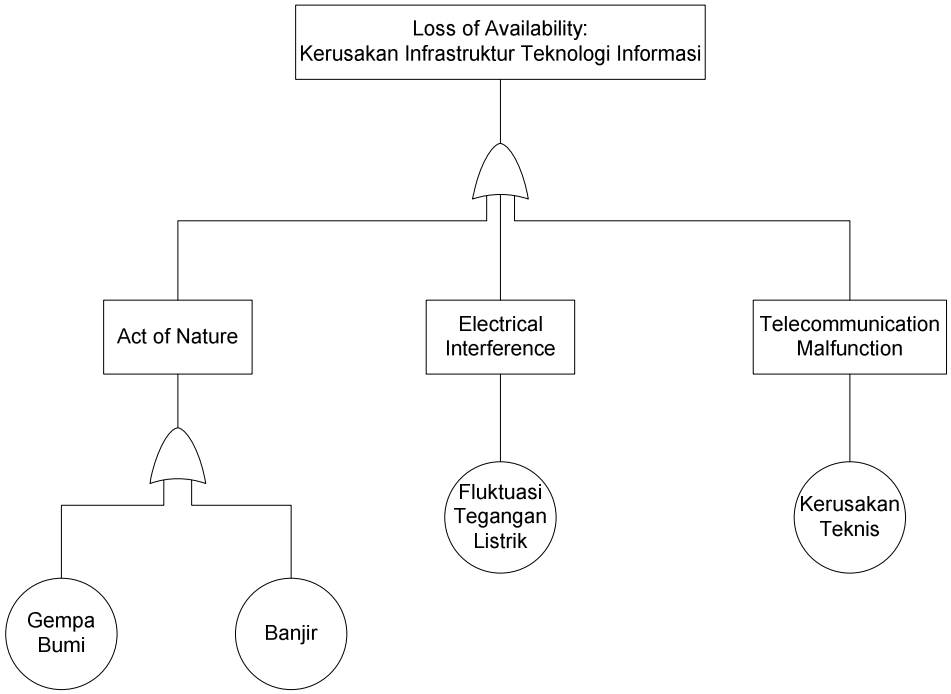
Sumber Ancaman	Kejadian	*Output*
Accidental disclosure	*1. Hacking* *2. Data Phising*	1. Penyalahgunaan data/informasi rahasia mengenai kegiatan PPM
Act of Nature	3. Gempa Bumi 4. Banjir	2. Menimbulkan kerusakan infrastruktur teknologi informasi
Alteration of Software	5. Kegagalan modifikasi aplikasi TI 6. Serangan virus dan	3. Menghambat akses aplikasi TI

Sumber Ancaman	Kejadian	*Output*
	malicious code	
Bandwith Usage	7. Penggunaan *bandwith* untuk akses jejaring sosial 8. Penggunaan *bandwith* untuk akses file multimedia	4. Mengurangi *bandwith* untuk mengakses aplikasi yang menunjang proses bisnis melalui internet
Electrical Interference/Disruption	9. Fluktuasi tegangan listrik	5. Menimbulkan kerusakan perangkat teknologi informasi
Intentional Alteration of Data	10. *Flooding Attack* 11. *Human error* dalam *approval* aplikasi keuangan 12. *Human error* dalam aplikasi proposal dan laporan	6. Munculnya *Denial of Service* (DoS) 7. Munculnya masalah dalam aplikasi TI
System Configuration Error (Accidental)	13. Kesalahan konfigurasi *operating system sever* 14. Kesalahan dalam konfigurasi jaringan	8. Menghambat akses informasi 9. Menghambat layanan teknologi informasi
Telecommunication Malfunction/Interruption	15. Kerusakan perangkat *server* 16. Kerusakan perangkat komputer 17. Kerusakan perangkat jaringan	10. Menghambat akses informasi
Human Resources	18. Kehilangan SDM TI dengan *critical knowledge/skill* 19. Penempatan SDM TI yang tidak kompeten	11. Menurunkan/menghambat kualitas layanan teknologi informasi

V. Analisa Risiko Teknologi Informasi

Mengacu kepada teknik analisa risiko teknologi informasi yang telah distandarisasi melalui dokumen ISO 31010, teknik yang digunakan untuk melakukan analisa risiko teknologi informasi dalam penelitian ini adalah **Fault tree analysis (FTA)**. FTA adalah teknik untuk mengidentifikasi dan menganalisis faktor-faktor yang dapat berkontribusi pada kejadian tertentu yang menyebabkan terjadinya risiko (biasanya didefinisikan sebagai kejadian puncak)[ISO31010]. Dalam analisa risiko dengan teknik *fault tree analysis*, faktor-faktor yang menjadi penyebab yang risiko diidentifikasi secara deduktif, diorganisasikan secara logis, kemudian digambarkan dalam sebuah diagram pohon yang menggambarkan faktor-faktor penyebab dan hubungan logis masing-masing kejadian terhadap kejadian puncak.
Tahap pertama dalam analisis risiko teknologi informasi menggunakan teknik *fault tree analysis* adalah menentukan kejadian puncak dalam risiko teknologi informasi,

kemudian menguraikan kejadian-kejadian apasaja yang berkaitan dengan kejadian puncak tersebut. Dalam kasus risiko teknologi informasi di lembaga penelitian perguruan tinggi, terdapat tiga kejadian puncak yang dapat menyebabkan risiko, yaitu kerusakan teknologi informasi, gangguan/hambatan aplikasi teknologi informasi, dan hilangnya integritas data (*loss of integrity*).

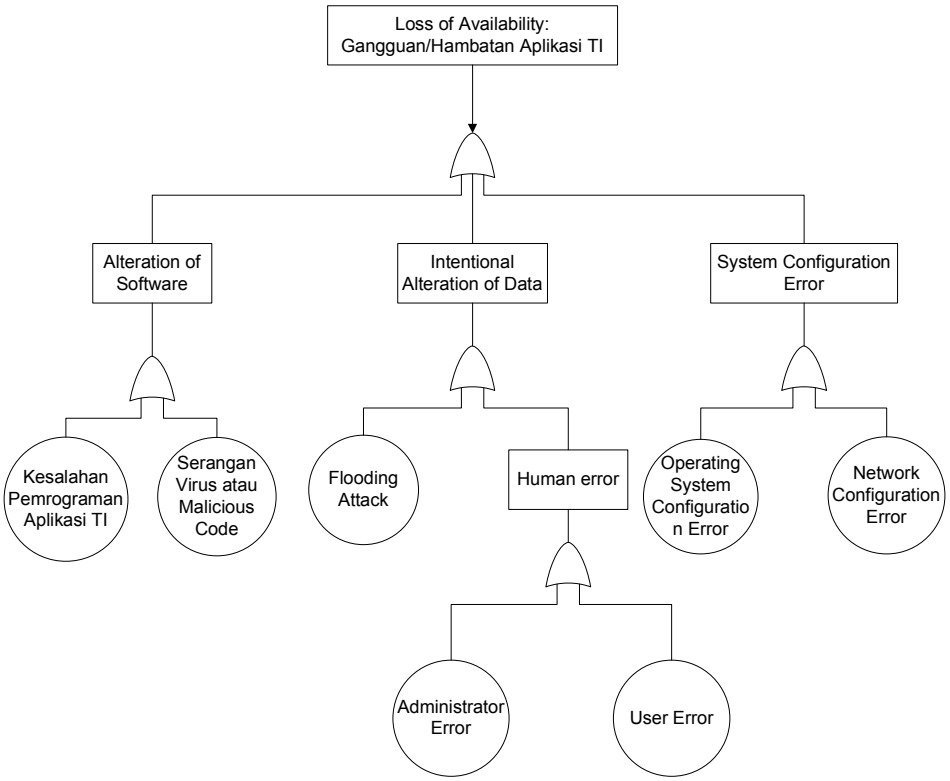


Gambar 1 Hasil Analisa Risiko dengan Kejadian Puncaknya adalah Kerusakan Infrastruktur TI LPPM

Gambar 1 di atas menunjukan analisis risiko dengan kejadian puncaknya adalah kerusakan infrastruktur teknologi informasi. Kerusakan dapat disebabkan oleh gangguan alam (*act of nature*), gangguan kelistrikan (*electrical interference*), atau gangguan telekomunikasi (*telecommunication malfunction*). Gangguan alam yang merupakan risiko teknologi informasi dapat disebabkan oleh gempa bumi atau banjir. Gangguan kelistrikan dapat disebabkan oleh fluktuasi tegangan listrik. Sedangkan gangguan telekomunikasi dapat disebabkan oleh kerusakan teknis dalam perangkat koneksi atau telekomunikasi.

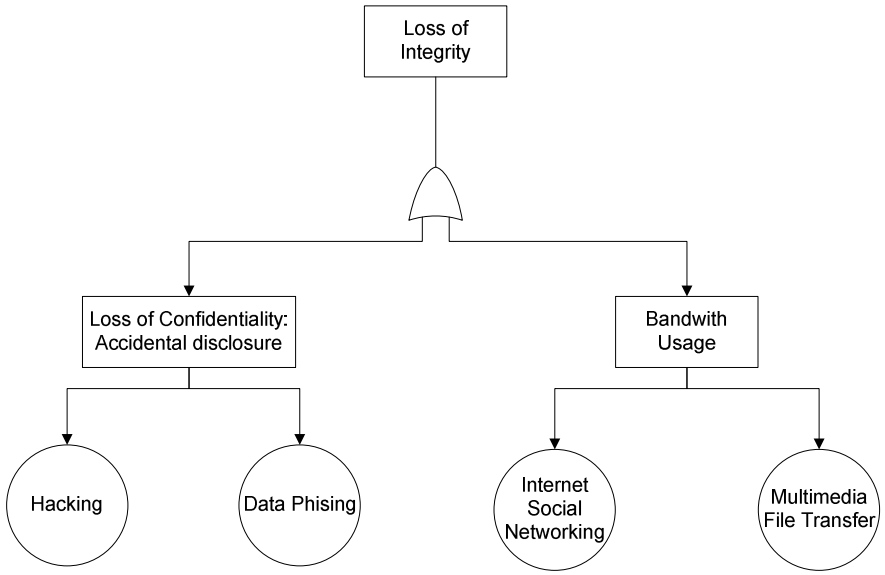
Gambar 2 di bawah ini menunjukan analisis risiko dengan kejadian puncaknya adalah gangguan aplikasi teknologi informasi. Gangguan aplikasi teknologi informasi dapat disebabkan oleh perubahan perangkat lunak (*alteration of software*), perubahan data (*alteration of data*), atau gangguan konfigurasi sistem (*system configuration error*).
Perubahan perangkat lunak dapat disebabkan oleh kesalahan dalam pengembangan aplikasi atau dapat juga disebabkan oleh serangan virus/malware. Perubahan data dapat disebabkan oleh banyaknya permintaan yang diterima oleh aplikasi sehingga menyebabkan *denial of service*, atau yang biasa disebut sebagai *flooding attack*. Perubahan data juga dapat disebabkan oleh kesalahan manusia (*human error*).

Kesalahan manusia dapat disebabkan oleh administrator atau oleh pengguna. Kesalahan konfigurasi sistem dapat disebabkan oleh kesalahan dalam konfigurasi sistem operasi (*operating system*), atau oleh kesalah konfigurasi jaringan (*network configuration error*).



Gambar 2 Hasil Analisa Risiko dengan Kejadian Puncaknya adalah Gangguan Aplikasi TI LPPM

Gambar 3 di bawah ini menunjukan analisis risiko dengan kejadian puncaknya adalah hilangnya integritas data. Hal tersebut dapat disebabkan oleh hilangnya kerahasiaan data atau penggunaan bandwith yang berlebihan sehingga menyebabkan sulitnya mengakses data.



Gambar 3 Hasil Analisa Risiko dengan Kejadian Puncaknya adalah hilangnya integritas organisasi

VI. Evaluasi Risiko Teknologi Informasi

Setelah seluruh risiko teknologi informasi di lembaga penelitian perguruan tinggi diidentifikasi dan dianalisa, maka risiko-risiko tersebut perlu dievaluasi. Evaluasi risiko perlu dilakukan untuk menentukan prioritas penanganan risiko. Evaluasi risiko dilakukan dengan mengacu kepada kriteria risiko yang telah ditetapkan sebelumnya.

Risiko dievaluasi berdasarkan kriteria risiko teknologi informasi yang telah ditentukan sebelumnya. Dengan mengacu kepada kriteria tersebut, tim manajemen risiko dapat mengkategorikan risiko dengan dampak yang tinggi, menengah, atau rendah. Serta mengevaluasi kemungkinan kejadiannya apakah tinggi, menengah, atau rendah.

Evaluasi dampak dan kemungkinan kejadian risiko juga dapat dianalisa melalui tabel berikut ini:

Tabel 5. Matriks Dampak Terhadap Kemungkinan Kejadian Risiko

Kemungkinan Kejadian	Dampak Risiko		
	Rendah	Menengah	Tinggi
Rendah	Rendah	Rendah	Tinggi
Menengah	Rendah	Menengah	Tinggi
Tinggi	Rendah	Menengah	Tinggi

Tabel 5 di atas menunjukan bahwa jika sebuah risiko memiliki kemungkinan kejadian yang rendah, namun memiliki dampak yang tinggi maka risiko tersebut dapat dikategorikan sebagai risiko tinggi. Contohnya kerusakan pada server.

Kejadian tersebut merupakan kejadian yang kemungkinannya rendah, mengingat kualitas server saat ini sangat baik dengan sistem garansi produsen yang baik. Namun jika risiko tersebut terjadi, akan memiliki dampak yang sangat siginfikasi terhadap implementasi teknologi informasi pada lembaga penelitian.

Sebaliknya, jika sebuah risiko memiliki kemungkinan yang sangat tinggi, namun memiliki dampak yang rendah, maka risiko tersebut dapat dikategorikan sebagai risiko yang rendah. Contohnya kesalahan manusia (*human error)* dalam penggunaan aplikasi keuangan kegiatan penelitian. risiko tersebut cukup sering terjadi, mengingat volume kegiatan penelitian yang dikelola oleh sebuah lembaga penelitian cukup banyak. Namun kejadian tersebut hanya akan berdampak terhadap satu transaksi keuangan saja. Sehingga tidak memiliki dampak yang signifikan terhadap teknologi informasi di lembaga secara keseluruhan.

VII. Perlakuan Risiko Teknologi Informasi

Beberapa strategi pemilihan dalam perlakuan risiko teknologi informasi diantaranya adalah[Tohidi11]:

1. Penerimaan Risiko (*Assumption of the risk*)
   Strategi perlakuan risiko dengan menerima risiko merupakan suatu strategi untuk menerima risiko, dan tetap menggunakan sistem serta teknologi informasi dengan diiringi upaya untuk tetap mengontrol risiko yang ada agar berada dalam batas yang dapat ditoleransi.
2. Menghindari Risiko (*Risk Avoidance*)
   Menghindari risiko adalah suatu strategi untuk mencegah terjadinya risiko dengan tidak melakukan kegiatan yang diperkirakan mempunyai risiko yang tidak dapat ditoleransi. Menghindari risiko juga dapat dilakukan dengan menghilangkan sumber ancaman yang dapat menyebabkan risiko.
3. Berbagi Risiko (*Risk Sharing/Transfer*)
   Berbagi risiko adalah strategi yang digunakan untuk memindahkan sebagian dari risiko ke individu, entitas bisnis, atau organisasi lain. Memindahkan risiko tidak berarti mengurangi tingkat kegawatan risiko, tetapi hanya memindahkan ke pihak lain dan harus disadari bahwa pada akhirnya dampak risiko tetap pada pemangku risiko utama (*principal risk owner*).
4. Mitigasi Risiko (*Risk Mitigation*)
   Mitigasi risiko adalah perlakuan risiko yang bertujuan untuk mengurangi risiko. Bentuk pengurangan risiko ini dapat berupa pengurangan kemungkinan terjadinya risiko, pengurangan kerugian yang diakibatkan bila risiko terjadi, dan diversifikasi risiko.

Berdasarkan alternatif pilihan perlakuan risiko tersebut di atas, *stakeholder* lembaga penelitian perguruan tinggi dapat mengklasifikasikan perlakuan risiko sesuai dengan alternatif strategi yang dipilihnya.

VIII. Kesimpulan

Manajemen risiko teknologi informasi di lembaga peneltian perguruan tinggi perlu dirumuskan sesuai dengan peranan teknologi informasi, dan karakteristik organisasi masing-masing lembaga. Perumusan manajemen risiko teknologi informasi berbasis ISO 31000 dilaksanakan melalui tahapan-tahapan penentuan konteks dan kriteria risiko, identifikasi risiko, analisa risiko, evaluasi risiko dan penentuan perlakukan risiko. Teknik yang digunakan untuk melakukan identifikasi, analisa dan juga evaluasi risiko sangat bergantung pada kondisi masing-masing lembaga dan juga ketersediaan data yang berkaitan dengan risiko teknologi informasi. Perlakuan risiko dapat dilaksanakan oleh lembaga penelitian perguruan tinggi dengan mengacu kepada beberapa alternatif perlakuan risiko teknologi informasi.

IX. Referensi

[1] Cresswell, J. W. (2003), Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Sage Publications.
[2] Segal, S (2011), Corporate Value of Enterprise Risk Management, John Wiley & Sons, Inc.
[3] Hamid Tohidi, The Role of Risk Management in IT systems of organizations, Procedia Computer Science 3 (2011) 881–887.
[4] International Standard , (2009) ISO 31000: Risk management — Principles and guidelines.
[5] Susilo J. & Krawu V., (2010) Manajemen Risiko berbasis ISO 31000 Industri Nonperbankan, PPM Manajemen.
[6] SANS Institute, *An Introduction to Information System Risk Management*, 2007
[7] International Standard, (2009), ISO 31010: Risk management – Risk assessment techniques.